XXVI НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ
МИНСК
КЗИ 2021
КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

МАТЕРИАЛЫ XXVI НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ

Минск | 25-27 мая 2021 года

Научно-производственное республиканское унитарное предприятие
"Научно-исследовательский институт технической защиты информации"

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXVI научно-практической конференции

Минск, 25-27 мая 2021 г.

Минск
Издатель Владимир Сивчиков
2021

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

Ответственный за выпуск –
заместитель директора по науке государственного предприятия «НИИ ТЗИ»,
канд. техн. наук, доцент *С. Н. Касанин*

К63 **Комплексная защита информации :** материалы XXVI науч.-практ. конф., г. Минск, 25-27 мая 2021 г. – Минск : Издатель Владимир Сивчиков, 2021. – 388 с.
ISBN 978-985-7030-87-3.

В сборнике представлены доклады ученых, специалистов, представителей государственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных направлений. Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-7030-87-3

ОРГКОМИТЕТ КОНФЕРЕНЦИИ

СОПРЕДСЕДАТЕЛИ

БЕЛОКОНЕВ Олег Алексеевич, Председатель комиссии Парламентского собрания Союза Беларуси и России по безопасности, обороне и борьбе с преступностью

ХРАМОВ Олег Владимирович, заместитель Секретаря Совета Безопасности Российской Федерации

ЧЛЕНЫ ОРГКОМИТЕТА

ГОРБАЧ Александр Николаевич, директор государственного предприятия «НИИ ТЗИ», Республика Беларусь

ЖЕРНОСЕК Сергей Васильевич, заместитель начальника Оперативно-аналитического центра при Президенте Республики Беларусь

ЗУБКОВ Артем Николаевич, директор Фонда содействия развитию безопасных информационных технологий; генеральный директор Медиа Группа «Авангард», Российская Федерация

КИРЮШКИН Сергей Анатольевич, советник генерального директора ООО «Газинформсервис», кандидат технических наук, Российская Федерация

КОНЯВСКИЙ Валерий Аркадьевич, заведующий кафедрой «Защита информации» МФТИ (ФизТех), научный руководитель ОКБ САПР, доктор технических наук, академик РАЕН и академик АЭН Российской Федерации

НОСКОВ Алексей Васильевич, консультант управления стратегического развития Министерства связи и информатизации Республики Беларусь

ЛЕНКОВ Алексей Александрович, Государственный пограничный комитет Республики Беларусь

ЛОСЬ Владимир Павлович, директор Центра исследования проблем кадрового обеспечения отрасли информационной безопасности РТУ МИРЭА, доктор военных наук, профессор, Российская Федерация

СИДОРОВ СЕРГЕЙ ВЛАДИМИРОВИЧ, начальник Центра защиты информации государственного объединения «Белорусская железная дорога»

ХАРИН Юрий Семенович, директор НИИ прикладных проблем математики и информатики БГУ, доктор физико-математических наук, член-корреспондент НАН Республики Беларусь

ЮЧКО ИВАН ПЕТРОВИЧ, Министерство обороны Республики Беларусь

ЯЗОВ ЮРИЙ КОНСТАНТИНОВИЧ, главный научный сотрудник ФАУ «ГНИИИ ПТЗИ ФСТЭК России», доктор технических наук, профессор, Российская Федерация

ПРОГРАММНЫЙ КОМИТЕТ

СОПРЕДСЕДАТЕЛИ

КОНЯВСКИЙ Валерий Аркадьевич, заведующий кафедрой «Защита информации» МФТИ (ФизТех), научный руководитель ОКБ САПР, доктор технических наук, академик РАЕН и академик АЭН Российской Федерации

ХАРИН Юрий Семенович, директор НИИ прикладных проблем математики и информатики БГУ, доктор физико-математических наук, член-корреспондент НАН Республики Беларусь

СЕКРЕТАРИ

КАСАНИН Сергей Николаевич, заместитель директора по науке государственного предприятия «НИИ ТЗИ», кандидат технических наук, доцент, Республика Беларусь

ЗУБКОВ Артем Николаевич, директор Фонда содействия развитию безопасных информационных технологий, генеральный директор Медиа Группа «Авангард», Российская Федерация

ЧЛЕНЫ ПРОГРАММНОГО КОМИТЕТА

БЕЛОВ Евгений Борисович, заместитель председателя Федерального УМО в системе высшего образования по УГСНП «Информационная безопасность», Российская Федерация

БОБОВ Михаил Никитич, главный специалист по защите информации ОАО «АГАТ – системы управления» – управляющая компания холдинга «Геоинформационные системы управления», доктор технических наук, профессор, Республика Беларусь

БОРБОТЬКО Тимофей Валентинович, заведующий кафедрой защиты информации БГУИР, доктор технических наук, профессор, Республика Беларусь

ГРИГОРЬЕВ Виталий Робертович, Заместитель директора по стратегическому развитию Института комплексной безопасности и специального приборостроения РТУ МИРЭА, кандидат технических наук, Российская Федерация

КУРИЛО Андрей Петрович, заведующий кафедрой международной информационной безопасности, ФГБОУ ВО МГЛУ, кандидат технических наук, доцент, Российская Федерация

КИРЮШКИН Сергей Анатольевич, советник генерального директора ООО «Газинформсервис», кандидат технических наук, Российская Федерация

КУРБАЦКИЙ Александр Николаевич, заведующий кафедрой технологий программирования БГУ, доктор технических наук, профессор, Республика Беларусь

КУЧИНСКИЙ Петр Васильевич, директор НИИ ПФП, доктор физико-математических наук, Республика Беларусь

ЛОСЬ Владимир Павлович, директор Центра исследования проблем кадрового обеспечения отрасли информационной безопасности РТУ МИРЭА, доктор военных наук, профессор, Российская Федерация

Выступление
Председателя комиссии Парламентского собрания Союза Беларуси и России по безопасности, обороне и борьбе с преступностью
Белоконева Олега Алексеевича
на открытии XXVI научно-практической конференции
«Комплексная защита информации»

Уважаемые организаторы, участники и гости конференции!

Нынешнее заседание – уже двадцать шестое по счету, но с годами проблема обеспечения комплексной защиты информации не становится менее актуальной.

Вызовы и угрозы, которые формируются в современной информационной сфере, без преувеличения представляют реальную опасность для конституционных основ и жизнедеятельности государств. Речь идет не только о манипулировании массовым сознанием, не только о дискредитации идеалов и ценностей, но и о более серьезных проблемах, вплоть до размывания национального суверенитета.

В этих условиях наши усилия должны быть направлены на обеспечение устойчивости информационной инфраструктуры наших стран. Вот почему в Приоритетных направлениях и первоочередных задачах дальнейшего развития Союзного государства на 2018–2022 годы, утвержденных постановлением Высшего Государственного Совета Союзного государства от 19 июня 2018 г. № 3, взаимодействие в сфере защиты информационных ресурсов Союзного государства и государств – участников Договора о создании Союзного государства стоит наравне с углублением военного и военно-технического сотрудничества.

Ответственно подходя к решению задач в сфере информационной безопасности, Беларусь и Россия совершенствуют механизмы противодействия возникающим угрозам, проводят совместные практические мероприятия, направленные на укрепление информационной безопасности и противодействие противоправной деятельности в информационном пространстве наших государств.

Уважаемые друзья!

Нам предстоит обмен мнениями, который, без сомнения, позволит предложить конкретные меры по совершенствованию системы обеспечения информационной безопасности, конструктивному взаимодействию, консолидации усилий и повышению эффективности защиты национальных интересов в информационной сфере.

Желаю конференции успешной работы на благо наших государств!

Приветствие
от заместителя Государственного секретаря –
члена Постоянного Комитета Союзного государства
Кубрина Алексея Александровича

Уважаемые участники конференции!

От имени Постоянного Комитета Союзного государства и от себя лично приветствую гостей и участников XXVI научно-практической конференции «Комплексная защита информации»!

Эта Конференция по праву является ведущей площадкой Союзного государства для обсуждения вопросов комплексной защиты безопасности научными, образовательными, производственными и государственными учреждениями государств – участников Договора о создании Союзного государства.

Практическое значение этой Конференции трудно переоценить.

Ее результаты широко используются в вопросах совершенствования информационной безопасности и систем защиты информации Беларуси и России и в иных смежных сферах деятельности Союзного государства.

Ярким примером тому могут являться уже успешно реализованные программы Союзного государства и реализуемая сегодня программа Союзного государства в области совершенствования системы защиты информационных ресурсов Беларуси и России в условиях геополитической обстановки, складывающейся вокруг этих государств.

Конференция, опираясь на широкий круг и квалификацию ее участников, позволяет обсудить и выработать в ходе дискуссий практические рекомендации и предложения для формирования проектов новых перспективных союзных программ.

Выражаю уверенность, что эта Конференция внесет достойный вклад в развитие информационных технологий и средств их защиты в государствах – участниках Союзного государства.

Желаю участникам Конференции успешной и результативной работы на благо Союзного государства.

Заместитель
Государственного секретаря –
член Постоянного Комитета
Союзного государства А. Кубрин

Приветствие
от заместителя Государственного секретаря Совета безопасности Республики Беларусь генерал-майора юстиции Рахманова Александра Александровича

Уважаемые коллеги, дорогие гости!

Научно-практическая конференция «Комплексная защита информации» – значимое ежегодное событие для профильных специалистов и ученых в области обеспечения информационной безопасности. Ее цель – детальное и всестороннее обсуждение на авторитетной экспертной площадке наиболее острых научных и организационно-правовых проблем кибербезопасности, обмен опытом и современными достижениями в этой самой быстро развивающейся сфере, демонстрация имеющегося потенциала и практических наработок при создании инновационных методов защиты информации.

Важное значение нынешнего мероприятия обусловлено не только стремительным техническим прогрессом, но и возникновением новых постоянно трансформирующихся рисков, вызовов и угроз в информационной сфере. Их эффективное предупреждение, выявление и пресечение невозможно без опережающего развития различных форм международного, регионального и межведомственного сотрудничества, направленного на изучение передового опыта построения и совершенствования проактивных систем защиты информации, подготовки и переподготовки профессиональных кадров. Активное интеграционное строительство в рамках Союзного государства показывает, что вопросы взаимодействия в данной сфере традиционно являются одними из самых востребованных среди населения и профессионалов, особенно с учетом внедрения в повседневную жизнь принципиально новых технологических решений. В этих условиях на первый план также выходит решение задачи по повышению информационной грамотности населения, формирование в обществе иммунитета от киберугроз. Кроме того, будем признательны за конкретные предложения по совершенствованию Концепции национальной безопасности Республики Беларусь, эта работа ведется по поручению Главы государства, данному на VI Всебелорусском народном собрании.

Желаю всем участниками и гостям конференции успехов в работе, интересных дискуссий и успешного решения поставленных задач, плодотворных творческих контактов.

Уверен, что итоги Конференции станут дополнительным импульсом для продвижения новых инициатив по поиску нестандартных и инновационных методов борьбы с киберинцидентами, повышения киберкультуры населения Союзного государства Беларуси и России.

Приветствие
от начальника Оперативно-аналитического центра
при Президенте Республики Беларусь
Павлюченко Андрея Юрьевича

Приветствие от начальника Оперативно-аналитического центра при Президенте Республики Беларусь

Уважаемые организаторы и участники конференции!

Примите искренние поздравления по поводу открытия XXVI научно-практической конференции «Комплексная защита информации»! Данный форум является одним из ведущих мероприятий Союзного государства, на котором обсуждаются проблемы обеспечения информационной безопасности, защиты информационных ресурсов, создания и применения эффективных средств и методов защиты информации.

В современных условиях значение защиты информации в обеспечении безопасности Союзного государства и успешного социально-экономического развития Беларуси и России непрерывно возрастает. Противоправное воздействие на информационно-коммуникационную инфраструктуру, информационные системы и ресурсы является одним из инструментов давления на государства.

Оперативно-аналитический центр при Президенте Республики Беларусь рассматривает настоящую конференцию как общепризнанное значимое мероприятие Союзного государства, на котором осуществляется обмен мнениями и выработка конструктивных предложений по решению организационных, правовых и технических проблем обеспечения защиты информации.

Конференция ежегодно собирает вместе ученых, представителей государственных органов, научных организаций и производственных предприятий.

Благодаря универсальному подходу к анализу проблем защиты информации, нацеленности на рассмотрение вопросов, имеющих практическую значимость, она по праву заслужила репутацию одной из важнейших инициатив по обеспечению информационной безопасности Союзного государства.

Выражаю уверенность, что результаты XXVI научно-практической конференции «Комплексная защита информации» станут важным ресурсом для государственных органов Республики Беларусь и Российской Федерации при подготовке предложений по реализации ими своих полномочий в области обеспечения безопасности в информационной сфере.

Желаю всем участникам конференции успехов, плодотворного обмена опытом и результативной работы!

Начальник
Оперативно-аналитического центра
при Президенте Республики Беларусь

А.Ю.Павлюченко

Приветствие от заместитель директора Федеральной службы по техническому и экспортному контролю России Куца Анатолия Владимировича

Уважаемые Олег Алексеевич и Олег Владимирович!
Уважаемые участники и организаторы XXVI научно-практической конференции «Комплексная защита информации»!

От имени Федеральной службы по техническому и экспортному контролю приветствую Вас по случаю начала работы конференции.

В настоящее время мировое сообщество охвачено стремительным внедрением информационных технологий во все сферы общественной жизни и государственного управления.

Результаты исследований отечественных и зарубежных аналитиков показывают, что объем глобального рынка информационных услуг и технологий ежегодно стремительно растет.

В этих условиях с точки зрения информационного пространства понятия «граница» и «территория государства» носит размытый характер, так как они становятся легко проницаемыми при использовании современных информационных технологий, а в условиях значимости используемых информационных ресурсов обуславливают возникновение рисков и формирование новых угроз в различных сферах деятельности общества и государства.

В настоящее время особо актуальным становится предотвращение использования информационных технологий для решения задач, противоречащих интересам обеспечения мира и стабильности, суверенитета, безопасности государства, безопасности граждан.

Анализ и прогнозирование развития разведывательных средств и систем специальных служб США и других стран НАТО показывают, что их активность, направленная на осуществление воздействия на информационные ресурсы России и Союзного государства, в целом не снижается, а только наращивается.

Продолжаются наращивание и совершенствование средств разведки, методы и способы добывания информации и воздействия на нее. Отдельные разведывательные средства объединяются в глобальные системы, способные, в случае непринятия мер защиты, обеспечить тотальный контроль по всему миру за обрабатываемой и передаваемой информацией.

При этом необходимо отметить, что значительное расширение областей использования современных информационных технологий вывели компьютерную разведку на одно из первых мест по значимости и объемам добываемой информации.

Основным целевым устремлением компьютерной разведки США и других стран НАТО являются государственные информационные системы, обрабатывающие информацию ограниченного доступа, а также различные открытые информационные системы и информационно-телекоммуникационные сети значимых объектов критически важной инфраструктуры.

Кроме того, отмечается нарастание угроз информационной безопасности со стороны преступных сообществ, как на национальном, так и на международном уровнях.

Очевидно, что в условиях масштабного возникновения новых угроз информационной безопасности поиск эффективных путей решения актуальных задач защиты информации в государственных информационных системах, в системах обеспечения безопасности значимых объектов критической инфраструктуры, персональных данных невозможен без объединения усилий и обмена лучшими практиками по защите информации на уровне взаимодействия специалистов Российской Федерации и Республики Беларусь.

Объединение усилий органов государственной власти, представителей бизнес-сообществ, научных и образовательных организаций будет способствовать созданию условий для развития и поддержки отечественных систем защиты информации Российской Федерации и Республики Беларусь, развитию безопасной информационной среды, подготовке кадров, соответствующих современным требованиям.

Организаторами проводимой сегодня научно-практической конференции в рамках запланированных секционных заседаний вынесены на обсуждение актуальные вопросы обеспечения защиты информации по различным направлениям.

Мы уверены, что представленные по ним доклады и выступления, обмен опытом и мнениями будут, не только интересны, но и позволят обсудить и определить оптимальные векторы развития и совместной работы в области обеспечения информационной безопасности.

Желаю участникам и организаторам научно-практической конференции «Комплексная защита информации» плодотворной работы, конструктивных дискуссий и достижения практических результатов, направленных на укрепление информационной безопасности Союзного государства и национальных систем обеспечения защиты информации.

Благодарю за внимание.

Приветствие
от Министра связи и информатизации Республики Беларусь
Шульгана Константина Константиновича

Министерство связи и информатизации Республики Беларусь приветствует участников XXVI научно-практической конференции «Комплексная защита информации» в столице Республики Беларусь городе Минске. Благодаря усилиям Постоянного Комитета Союзного государства и Парламентского Собрания Союза Беларуси и России, конференция стала уже традиционной и собирает известных ученых, высококвалифицированных специалистов в области защиты информации.

События, происходящие в мире, указывают на актуальность для государств – участников Союзного государства таких задач и направлений деятельности как:

обеспечение защищенности персональных данных с использованием перспективных высоких технологий;

подготовка кадров в области информационной безопасности;

техническое, информационное и нормативно-правовое совершенствование трансграничного взаимодействия Беларуси и России;

внедрение средств защиты информации, разработанных в Беларуси и России в рамках выполнения мероприятий программы Союзного государства.

В Республике Беларусь, как и в Российской Федерации, создана надежная система, позволяющая эффективно противодействовать вызовам, угрозам вмешательства во внутренние дела наших суверенных государств в информационной среде. Уверен, что между участниками конференции состоится плодотворный обмен опытом в области разработки и внедрения теоретических, методологических, нормативных, организационно-технических, правовых и гуманитарных вопросов обеспечения информационной безопасности. Решения, принятые по итогам конференции, будут способствовать выработке единого подхода по вопросам использования защищенных информационных технологий в различных сферах жизнедеятельности государств – участников Союзного государства и общества в целом на всех этапах развития интеграционных процессов России и Беларуси.

Министр связи и информатизации  К.К. Шульган

Приветствие от Председателя Государственного комитета по науке и технологиям Республики Беларусь Шумилина Александра Геннадьевича

Уважаемый Алексей Александрович!
Уважаемые участники конференции!

Я рад приветствовать гостей и участников XXVI научно-практической конференции «Комплексная защита информации»!

Эта конференция имеет важное значение для наших союзных государств, являясь платформой для обсуждения и поиска решений актуальных вопросов комплексной защиты информации как в государственном секторе, так и во множестве организаций реального сектора экономики.

В Концепции национальной безопасности Республики Беларусь информационная сфера рассматривается в качестве одной из основных сфер национальной безопасности. Основное направление развития страны в этом направлении на ближайшую пятилетку заданы в утвержденных Президентом приоритетных направлениях научной, научно-технической и инновационной деятельности на 2021–2025 годы. Это приоритет 1 «Цифровые информационно-коммуникационные и междисциплинарные технологии, основанные на них производства» и приоритет 6 «Обеспечение безопасности человека, общества и государства». В рамках реализации данных приоритетов утверждены перечень соответствующих государственных научно-технических программ: ГНТП «Цифровые технологии и роботизированные комплексы»; ГНТП «Кибербезопасность».

Прошедший год и усложнившаяся эпидемиологическая ситуация во всем мире поставили перед нами новые вызовы, требующие изменения в подходе к работе, обеспечении информационной безопасности как на государственном уровне, так и на уровне конкретных организаций. Для множества частных компаний, а также части государственных организаций, домашний офис стал офисом для тысяч сотрудников. Исследования, проводимые «Лабораторией Касперского» показали, что почти три четверти сотрудников компаний по всему миру хотели бы сохранить возможность гибридного подхода к выполнению своей работы и в будущем. Поэтому реализация мероприятий по обеспечению кибербезопасности никогда не были так важны, как на сегодняшний день. Но при этом они должны быть понятными, актуальными и применимы в реальной жизни за пределами офиса.

Отмечу, что по итогам 2020 года почти 40 % корпоративных организаций подверглись целевым кибератакам.

По экспертным оценкам в целом, суммарный ущерб от нападений только лишь программ-шифровальщиков в 2020 году превысил 1 млрд, долларов, а общемировой урон от киберпреступлений в 2021 году может достигнуть 6 триллионов долларов или 190 тысяч долларов в секунду.

Ущерб от киберпреступности в 2020 году в России достиг почти 70 млрд рублей, а в текущем году он может возрасти почти на треть и составить 90 млрд рублей.

В 2020 году на территории нашей страны было зафиксировано более 25 тысяч киберпреступлений (25 575), а всего годом ранее эта цифра была на уровне

10 тысяч (10 567). Их удельный вес в общем объеме зарегистрированных преступлений возрос с 12 до 26,8 %.

И в этом году количество киберпреступлений продолжает расти. Только за январь-февраль текущего года было зафиксировано более 4000 киберпреступлений. Для сравнения: за аналогичный период прошлого года в Беларуси их было около 1 000.

При этом наиболее распространенные способы совершения киберпреступлений в кредитно-финансовой сфере – фишинг (подделка сайтов, аккаунтов), вишинг (телефонное мошенничество с применением методов социальной инженерии), взлом учетных записей пользователей с использованием вредоносных программ.

Только за 2020 год жертвами киберпреступлений стали почти 100 тысяч граждан Беларуси, персональные данные которых стали известны злоумышленникам.

Вместе с тем, государству удалось не только достойно выдержать, но и пресечь многие попытки злоумышленников. Такой результат достигнут благодаря организованной и проведенной на государственном уровне за последние 5 лет работе в области информационной безопасности по таким направлениям как совершенствование правового регулирования, разработка новых методов и технологий защиты информации, внедренных сегодня практически во все сферы деятельности, совершенствование телекоммуникационной инфраструктуры и многое другие.

Однако для противодействия возрастающим информационным угрозам необходимо и дальше развивать и совершенствовать технологии и методы борьбы с киберпреступностью. При этом первостепенное значение имеет необходимость более глубокого анализа и моделирования угроз, а также более активного подхода к обнаружению угроз и реагированию на них.

Общество 21 века как никогда нуждается в развитии средств и систем охраны информационного пространства. Выстраивание уникальной системы информационной защиты государства в современных условиях требует не только новых умений, но и нового уровня международного сотрудничества. Очевидно, что мы имеем дело с проблемой глобального характера, которая выходит далеко за рамки компьютерных систем и вообще технической сферы.

Как отметил Глава государства Александр Григорьевич Лукашенко «...Беларусь, будучи вовлеченной в глобальные информационные процессы, не будет прятаться, а будет учиться бороться в этом водовороте, чтобы остаться независимой».

Уважаемые коллеги, участники конференции!

Я надеюсь, что сегодняшнее мероприятие позволит нам сделать очередной шаг в сторону высокотехнологического безопасного пространства двух братских государств: Беларуси и России.

Желаю всем успешной, плодотворной работы и успехов в достижении намеченных целей!

Председатель Государственного
комитета по науке и технологиям
Республики Беларусь А. Г. Шумилин

Приветствие
от председателя Государственного пограничного комитета Республики Беларусь
Лаппо Анатолия Петровича

Уважаемые участники конференции!

Обеспечение информационной безопасности стало одной из глобальных проблем, с которой столкнулось современное общество. Интернет, компьютеры, телефоны, планшеты и т.п. стали неотъемлемой частью жизни, значительно упростив ее. С другой стороны, информационные технологии, все больше проникая во все сферы жизни общества, порождают новые риски, вызовы и угрозы, которые напрямую затрагивают вопросы обеспечения национальной безопасности, в т.ч. защищенность информационной инфраструктуры, информационных систем и ресурсов.

Функционирование военных объектов, промышленности, транспорта, энергетики, электросвязи, здравоохранения тесно связанно с автоматизированными системами управления и находится в прямой зависимости от их надежности и защищенности.

И органы пограничной службы Республики Беларусь не являются исключением. По мере все более широкого внедрения современных информационных систем и средств контроля в повседневную деятельность пограничников растет понимание важности обеспечения их стабильной работы и осознание значимости проблемы защиты информации.

Мы прекрасно представляем всю сложность организации противодействия разработке и распространению средств уничтожения, блокирования, модификации и похищения информации. Поэтому для эффективного решения задач в обеспечении информационной безопасности важно постоянное взаимодействие между заинтересованными структурами и тесная взаимосвязь науки и практики.

Уважаемые участники! Уверен, что в ходе конференции удастся обсудить значительный спектр проблемных вопросов в сфере обеспечения комплексной защиты информации, ознакомиться с передовым опытом по их решению.

Желаю всем успешной и плодотворной работы!

С уважением,

Председатель Государственного пограничного комитета Республики Беларусь генерал-лейтенант

А. П. Лаппо

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

АКТУАЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОЮЗНОМ ГОСУДАРСТВЕ

УДК 004.056

О ЗАРУБЕЖНОМ ОПЫТЕ ФУНКЦИОНИРОВАНИЯ ЦЕНТРОВ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

В.Ю. АРЧАКОВ, А.Л. БАНЬКОВСКИЙ, Е.В. ЗЕНЧЕНКО
Государственный секретариат Совета Безопасности Республики Беларусь

В условиях цифровой трансформации, сопровождающейся усложнением информационных систем, безопасность, а также работоспособность и отказоустойчивость инфраструктур стала крайне актуальной темой для современного общества. Как результат, склонность к авариям и ошибкам в ходе настройки и эксплуатации, а также атаки на критически важные объекты информатизации (КВОИ), построенные с использованием современных технологий, ведут к появлению новых вызовов и угроз национальной безопасности любой страны.

В соответствии с общей классификацией центры реагирования бывают государственными, общественными и коммерческими. [1] Несмотря на имеющийся правовой статус **государственные центры**, как правило, инертны, удалены от интересов отдельных организаций, забюрократизированы и имеют недостаточное финансирование. Отсутствие у **коммерческих CERT (CSIRT)** необходимого административного ресурса стимулирует к нахождению различных моделей сотрудничества с правоохранительными и регулирующими органами. **Общественные** CERT часто не обладают достаточной компетенцией и опытом, но при этом их услуги более доступны и часто бесплатны.

В **международном формате** в целях выработки основ правового режима обеспечения кибербезопасности в рамках ООН сформирована группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникации в контексте международной безопасности. В целом предлагаемые ею меры укрепления доверия в киберпространстве в контексте реагирования на инциденты предусматривают также создание механизмов и процессов по консультациям и обсуждению инцидентов, подготовку соответствующего национального законодательства как основы кооперации в сфере обеспечения международной информационной безопасности, создание национальных и совместных групп реагирования на чрезвычайные ситуации в киберпространстве, развитие партнерства государственного и частного секторов с разработкой механизмов по обмену передовым опытом в сфере информационной безопасности.

На **региональном** уровне в ***НАТО*** с 2013 года функционирует единая система для своевременного выявления и нейтрализации киберугроз, а при необходимости и восстановления работоспособности компьютерных сетей органов управления стран-участниц. Основными ее элементами являются центры по реагированию на компьютерные инциденты, развернутые при штаб-квартире НАТО (г. Брюссель, Бельгия) и при штабе стратегического командования операций ОВС блока (г. Монс, Бельгия). Проверка эффективности системы реагирования на компьютерные угрозы проводится на всех крупных мероприятиях оперативной и боевой подготовки объединенных вооруженных сил альянса.

Европейское агентство по сетевой и информационной безопасности (ENISA) работает в тесном сотрудничестве с государствами – членами ***ЕС***. Эффективность взаимодействия значительно повышается за счет использования центров обмена информацией и анализа (ISAC) и государственно-частных партнерств (ГЧП). Наибольшее распространение получили

контрактные ГЧП-проекты, связанные с предоставлением специализированных услуг аутсорсинга частных операционных центров безопасности (SOC) по мониторингу и реагированию на инциденты информационной безопасности, а также центров обмена и анализа информации о киберугрозах и других профильных центров компетенции в сфере информационной безопасности. В марте 2019 года Европол объявил о принятии нового протокола экстренного реагирования правоохранительными органами стран ЕС на крупные трансграничные кибератаки, подобные эпидемиям известных компьютерных вирусов WannaCry и NotPetya. За его реализацию отвечает Европейский центр по борьбе с киберпреступностью (EC3).

Некоторая систематизация сотрудничества по реагированию на киберинциденты в ***Организации Договора о коллективной безопасности (ОДКБ)*** произошла в 2014 году с созданием Консультационного координационного центра по вопросам реагирования на компьютерные инциденты (ККЦ)**.** ***В*** рамках взаимодействия государств-членов ОДКБ летом 2019 года впервые проведена командно-штабная тренировка по реагированию на различные типовые угрозы. Для дальнейшего совершенствования на практике отработаны вопросы о сроках и форматах передачи данных с выявлением проблемных моментов.

На **национальном уровне** в ***США*** руководящая роль по немедленному реагированию на киберинциденты отведена совместной национальной оперативной группе киберрасследований под эгидой ФБР. При этом Национальный центр кибербезопасности и интегрированных коммуникаци (NCCIC) координирует действия по помощи пострадавшим организациям и поиску «сетевого агрессора», а Национальный центр интеграции разведки по киберугрозам (CTIIC) руководит процессом определения стратегий по предотвращению и преодолению угроз. Среди разнообразных некоммерческих организаций (НКО) – т. н. центров компетенции, предоставляющих услуги в сфере оценки кибербезопасности и обмена опытом реагирования на киберугрозы возможно выделить центр обмена и анализа информации о финансовых услугах (FS-ISAC), национальный альянс киберэкспертизы и обучения (NCFTA), EnergySec (некоммерческая корпорация США поддержки безопасности критически важных технологических инфраструктур организаций энергетического сектора).

Образованный в феврале 2017 года на основе профильных подразделений МИ-5 и штаб-квартиры правительственной связи Национальный центр кибербезопасности (NCSC) призван укрепить систему реагирования на киберинциденты и обеспечить лидирующее положение ***Великобритании*** в данной сфере на международной арене. Помимо этого, Центр защиты национальной инфраструктуры и Национальное техническое ведомство по обеспечению информационной безопасности (CESG) разработали две «Схемы реагирования на киберинциденты» (CIR), призванные оказать содействие критически важным инфраструктурным компаниям получать услуги, которые бы в точности соответствовали их потребностям, а также предоставить списки специализированных сертифицированных компаний, способных оказать содействие в преодолении кризисных ситуаций. Подобный подход позволил жертвам кибератак получить необходимую помощь, одновременно предоставляя возможность Центру правительственной связи и Центру защиты национальной инфраструктуры сконцентрироваться на тех кибератаках, которые представляют наибольшую угрозу национальной безопасности [2]. Как совместная инициатива бизнеса и правительства Великобритании в 2013 году для британских компаний под эгидой CERT-UK создано Партнерство по обмену информацией в области кибербезопасности (CiSP). Партнерство финансируется Национальной программой кибербезопасности и объединяет организации различных масштабов из самых разных секторов. Проект CiSP получил международное признание и стал своего рода стандартом для других стран.

Во ***Франции*** ANSSI, являясь основным координирующим органом обеспечения кибербезопасности, действует в качестве правительственной группы реагирования на чрезвычайные ситуации, которая также предоставляет рекомендации и советы в области защиты и устойчивости общественных сетей и важнейших элементов инфраструктуры. Оперативный центр безопасности информационных систем (COSSI) входит в структуру ANSSI и несет исключительную ответственность за определение и предотвращение кибератак против государственных информационных систем [3].

В ***Германии*** создан CERT-Verbund – альянс различных немецких государственных CSIRT (CERT-Bund, военная CERTBw и несколько CERT федеральных земель), частных CSIRT крупнейших компаний и CSIRT частных поставщиков продуктов и услуг в области информационной безопасности. Каждый центр реагирования отвечает за собственную аудиторию, однако участники альянса обмениваются информацией и поддерживают друг друга при разрешении инцидентов [4]. При этом важнейшей частью их функционирования является статистическая оценка совместно используемых данных и предоставление информации для стратегического анализа. Помимо этого, реагирование на инциденты в информационной сфере в Германии осуществляется в рамках проекта UP KRITIS, объединяющего опыт государственного и частного сектора и способствующего сотрудничеству в интересах повышения кибербезопасности критической инфраструктуры в Германии.

В ***Италии*** частные компании-поставщики информационных услуг и операторы элементов инфраструктуры как на национальном, так и на общеевропейском уровне, обязаны информировать отдел кибербезопасности (NSC) обо всех значимых нарушениях и взломах их сетей, а также предпринимать требуемые меры для обеспечения кибербезопасности. NSC имеет право созвать Межминистерский ситуационно-плановый отдел по вопросам киберкризисов в случае, если киберинцидент несет угрозу национальной безопасности либо имеет такой масштаб, что требует координации действий для его преодоления. Кроме того, компании, частично находящиеся в собственности государства, такие как ENEL (энергосети), ENI (нефтегазовая промышленность), Poste Italiane (почта Италии), ENAV (контроль авиаперевозок), TrenItalia (железная дорога) и Центральный банк Италии подписали соглашения о сотрудничестве с Департаментом информации и безопасности о добровольном информировании о попытках взлома и обмене данными в области безопасности [5].

Согласно подходам ***Норвегии*****,** главная ответственность за обеспечение информационной безопасности возлагается на владельцев или операторов информационных инфраструктур. При этом затраты на ее обеспечение должны быть сопоставимы с рисками.

В 2014 году в ***Китае*** создана Центральная руководящая группа по кибербезопасности и информатизации во главе с председателем КНР. В составе группы выделена Государственная канцелярия по делам Интернета, именуемая в международном экспертном сообществе как Администрация по киберпространству КНР. Понимая, что даже самому большому в мире аппарату исполнительной власти не по силам обеспечить полный контроль за интернет-пространством, в КНР частично передоверяют реализацию систем сетевой безопасности операторам, которые, в свою очередь, «должны соответствовать требованиям системы защиты уровня безопасности сетей и другим требованиям, выполнять обязательства, обеспечивать работу сетей без вмешательств, препятствовать доступу разрушающих или несанкционированных запросов, утечке данных, их хищению и фальсификации».

В ***России*** заложен основательный фундамент для дальнейшего практического совершенствования и предоставления дополнительных полномочий государственным органам по реагированию на инциденты. Согласно Федеральному закону о безопасности критической информационной инфраструктуры России на значимых объектах критической информационной инфраструктуры и в сетях электросвязи установлены технические средства государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы (ГосСОПКА). Данная система объединяет ведомственные и территориальные центры обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также Национальный координационный центр по компьютерным инцидентам (НКЦКИ), который организует обмен информацией о них с госведомствами и юрлицами, владеющими объектами критической инфраструктуры, операторами связи, иностранными госорганами.

Таким образом, анализ мировой практики обеспечения информационной безопасности показывает, что деятельность зарубежных государств по реагированию на киберинциденты, осуществляется комплексно и целенаправленно сразу по нескольким направлениям – государственному, коммерческому и общественному. Несмотря на некоторые различия в подходах, их объединяет создание целостной системы реагирования на инциденты, соче-

тающей правовые, организационные и технические меры защиты с использованием современных методов прогнозирования, анализа и моделирования ситуаций, в том числе с использованием передовых технологий искусственного интеллекта. Обращает на себя внимание подход, при котором формируется разветвленная структура национальной сети команд оперативного реагирования, включающая отраслевые и коммерческие центры, что способствует оперативности и гибкости при принятии решений. Более того, такая структура характеризуется развитием и углублением компетенции и специализации. При этом ключевая задача на государственном уровне – максимально возможное исключение дублирующих функций, а также стандартизация и совместимость методик их работы.

Характерными современными тенденциями также можно считать направленность на создание механизмов взаимодействия на двустороннем, региональном и международном уровнях, выработку мер (технических, правовых, дипломатических и др.) по защите критической инфраструктуры от киберугроз и реагирование на них, постоянное совершенствование национального законодательства, развитие государственных структур, ответственных за обеспечение кибербезопасности и обмен информацией, обеспечение сферы кибербезопасности высококвалифицированными кадрами (именно такой подход закреплен и в Концепции информационной безопасности Республики Беларусь [6]).

Целесообразно обратить внимание на новую тенденцию отказа от распределенной децентрализованной системы в пользу большей централизации усилий в одном органе с отраслевыми структурами. В большинстве зарубежных стран центры реагирования функционируют при соответствующих силовых структурах, отвечающих за информационную безопасность, и определены как основные точки управления инцидентами и развития коммуникации в рамках международных специализированных площадок. При этом наибольшее внимание уделяется развитию партнерства государственного и частного секторов с разработкой механизмов по обмену передовым опытом в сфере информационной безопасности, координации реагирования на угрозы. А основные усилия направлены на использование научно-экспертного потенциала для развития и совершенствования нормативной правовой базы, выработки единого понятийно-категориального аппарата в области профилактики, проведения расследований и минимизации последствий киберинцидентов.

Проведенный сравнительно-правовой анализ показывает, что система реагирования на киберинциденты в Республике Беларусь частично аккумулирует в себе лучшие зарубежные практики, в том числе обмен информацией о кибератаках и киберугрозах через деятельность национальных и международных центров реагирования на компьютерные инциденты, работа в тесном контакте с региональными и международными объединениями CSIRT/CERT (FIRST, Trusted Introducer). В то же время в Беларуси пока не нашел применения зарубежный опыт реализации общественных и коммерческих центров реагирования на инциденты информационной безопасности. Тем более, что государственные CERT, функционирующие на базе спецслужб, иногда воспринимаются среди населения и бизнес-сообщества с некоторой опаской, а за рубежом – с недоверием.

В этой связи представляется важным изучить имеющийся значительный потенциал общественных и отраслевых центров реагирования, развитие государственно-частного партнерства при определяющей роли национального регулятора. Как показывает зарубежный опыт, это позволяет снять с государства часть ответственности за обеспечение кибербезопасности, распределить обязанности по развитию соответствующей инфраструктуры на все субъекты информационных отношений, а также повысить доверие к государственной системе реагирования не только среди национального бизнес-сообщества, но и на международной арене. Дополнительным позитивным фактором от интеграции в международные и региональные структуры CERT (CSIRT) может стать повышение привлекательности Беларуси как безопасной площадки для развития IT-индустрии.

Не менее важным видится и продолжение теоретико-прикладных исследований в данной одной из наиболее динамично развивающейся сфере национальной безопасности, так как отставание здесь зачастую равноценно утрате уже имеющихся позиций, а развитие интеллектуальной и образовательной компоненты остается приоритетом для любого государства.

Эти и иные факторы обуславливают необходимость их **учета при совершенствовании существующих документов стратегического планирования**. Как известно, на VI Всебелорусском народном собрании Глава государства дал **поручение обновить действующую Концепцию национальной безопасности** [7]. С учетом значимости, многоаспектности и всепроникающего характера новых рисков, связанных с обеспечением информационной безопасности, жизненно важным представляется придание процессу ее обеспечения более комплексного, скоординированного и упреждающего характера. Важно изучить необходимость ревизии существующей системы реагирования на риски, вызовы и угрозы национальной безопасности, обеспечить обратную связь с гражданским и научным сообществами и коммерческим сектором, придать применяемым мерам проактивный (упреждающий) характер.

Список литературы

1. CSIRT Setting up Guide in English [Электронный ресурс] // ENISA. – Режим доступа : https://www.enisa.europa.eu/publications/csirt-setting-up-guide/atdownload /fullReport/. – Дата доступа : 25.04.2021/

2. Киберготовность Соединенного королевства: краткий обзор [Электронный ресурс] // Потомакский Институт политических исследований. – Режим доступа : https://analytica.digital.report/wp-content/uploads/2017/05/CRI-UK-RU.pdf. – Дата доступа : 24.03.2021.

3. Франция и киберпреступность [Электронный ресурс]. – Режим доступа: https://www.diplomatie.gouv.fr/ru/politique-etrangere/securite-desar-mement-et-non-proliferation/ lutter-contre-la-criminalite-organisee/la-france-et-la-cyber-securite/. – Дата доступа: 02.03.2021.

4. Der CERT-Verbund ist die Allianz deutscher Sicherheits- und Computer-Notfallteams mit heute über 40 Mitgliedern [Электронный ресурс] // CERT-Verbund. – Режим доступа : https://www.cert-verbund.de/. – Дата доступа : 20.04.2021.

5. Индекс киберготовности Италии 2.0 – Часть 6 : Обмен информацией / Мелисса Хатауэй [Электронный ресурс] // Digital.report. – Режим доступа : https://digital.report/ kibergoto-vnost-italii-2-0-obmen-informatsiey/. – Дата доступа : 25.03.2021.

6. Концепция информационной безопасности Республики Беларусь [Электронный ресурс] : пост. Совета Безопасности Респ. Беларусь, 18 марта 2019 г № 1 // Официальный Интернет-портал Президента Респ. Беларусь. – Режим доступа : https//:www.president.gov.by. – Дата доступа : 21.04.2021.

7. Об утверждении Концепции национальной безопасности Республики Беларусь : Указ Президента Респ. Беларусь, 9 ноября 2010 г., № 575 // Национальный реестр правовых актов Республики Беларусь. 2010 г., № 276, 1/12080.

УДК 004.5, 004.7, 334.024, 338.2

СЕТЬ ИНТЕРНЕТ КАК ОПРЕДЕЛЯЮЩИЙ КОМПОНЕНТ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОГО РАЗВИТИЯ И КЛЮЧЕВАЯ УГРОЗА БЕЗОПАСНОСТИ

А.А. КОСОВСКИЙ, И.В. МАТВИЕНКО, Т.В. ШЛЫЧКОВА, Н.Г. ЮНЕВИЧ
Государственный комитет по науке и технологиям Республики Беларусь,
Государственное учреждение «Белорусский институт системного анализа и информационного обеспечения научно-технической сферы»
г. Минск, Республика Беларусь

Возможности коммуникаций, которые стали доступны государствам, юридическим и физическим лицам после возникновения глобальной сети Интернет, привели к кардинальному преобразованию общества и его экономической реальности. Интернет сегодня – это среда, используемая для всевозможных форм взаимодействия всех субъектов экономики. Высокая степень необходимости интернета как в повседневных практиках общества, так и в деятельности государства и бизнес-сообщества, воздвигает его в ряд необходимых элементов социально экономического развития общества. Уже на 31 декабря 2020 года в мире числилось более 5 млрд пользователей сети Интернет – это 64,2 % от общего населения Земли [1].

Приоритетную важность представляет собой переход различных государственных отраслей экономики в цифровое пространство – электронное правительство. Предоставление цифровых услуг населению, создание государственных информационных систем и ресурсов, формирование межгосударственных каналов передачи данных сегодня представляют собой повсеместные практики.

На текущий момент 80 % организаций, прошедшие стадию цифровых преобразований (внедрение технологий «Индустрия 4.0»: промышленный интернет вещей, большие данные, 3D-принтеры и др.), смогли существенно увеличить свою прибыль. Ежегодная прибыль компаний Samsung, LG, Huawei и др. оценивается в десятки млрд долларов США, что демонстрирует не только успешность цифровизации бизнес-процессов компаний, но и актуальность разрабатываемой ими продукции – технических средств и средств связи [2].

Сеть интернет позволила сформировать новый рынок цифровых услуг и оказала значительное влияние на финансовое благосостояние стран. Так возникла экономика совместного использования (Sharing economy) – переход к платформенным решениям. Изначально базирующиеся на цифровых рынках платформы «Google», «Facebook» (США), «Amazon» (США), «Uber» (США), «Alibaba» (Китай), «Яндекс» (Россия) являются гигантами цифрового мира и имеют исключительное конкурентное преимущество как на глобальном, так и на местном уровне [3, 4]. При этом развитие индустрии цифровых денег (криптовалют) оценивается в 2021 году 1,41 трлн $ (рис. 1).

В современных реалиях цифровая экономика стала мощным фундаментом развития государств: страны с более развитой цифровой экономикой получают большую долю своего ВВП за счет высокотехнологичных секторов. Предполагается, что к 2025 году цифровая экономика может достичь показателя в 50 % глобального ВВП, а в развитых странах превысить его.

Иллюстрирование объемов капитализации цифровых компаний, построенной на монетизации цифровых массивов данных, а также анализ вклада цифровой экономики в ВВП, позволяют выявить следующую парадигму – данные сегодня выступают ключевым нематериальным активом экономики, а киберугрозы главным образом ориентированы на их хищение, т. е. на несанкционированный доступ к компьютерной системе или сети и краже личных, конфиденциальных и финансовых данных.

Киберугрозы сегодня нацелены на все области, использующие цифровые данные: здравоохранение, образование и науку, банковскую сферу, государственные органы, представителей бизнеса и многое другое. В большинстве случаев цель злоумышленников – хищение персональных данных: номера банковских счетов и кредитных карт, паспортные дан-

ные, медицинские карты, данные об объектах интеллектуальной собственности, а также информация, относящаяся к государственной, коммерческой и военной тайне.

Рис. 1. Рыночная стоимость ключевых цифровых компаний, млрд

При рассмотрении области киберугроз на уровне государств можно заметить, что кибератакам подвержены как страны с высоким уровнем экономического развития (США, Китай, Канада и т. п.), так и с низким уровнем [5].

На текущий момент основными видами атак, подпадающими под понятие киберугрозы, являются: киберфизические атаки, вредоносное программное обеспечение (включая программы-вымогатели, rootkit, backdoor, троянские программы, шпионские программы, и т. п.), DDoS-атаки (потоки ложных запросов) и ботнеты (компьютерные сети), социальная инженерия (в т.ч. фишинг) и т. п.

Данные инструменты применительны практически ко всем сферам деятельности государства, бизнесу и общественной жизни. Наиболее актуальными угрозами можно считать:

– социальная инженерия – это технологии манипулирования людьми в сети Интернет. В основном злоумышленники пытаются завоевать доверие жертвы и спровоцировать действия, нарушающие методы безопасности (раскрытие конфиденциальной информации или предоставление доступа к важным ресурсам). В 2020 году, например, злоумышленники получили доступ к логинам и паролям известных личностей в Twitter через сотрудников социальной сети, а позже призвали людей переводить деньги на мошеннические счета;

– DDoS-атаки или отказ от обслуживания – это поток ложных запросов, блокирующих ресурс. DDoS-атаки исходят из распределенных или множественных источников, или IP-адресов. Наиболее частый вариант развития подобных атак – замедление работы Интернет-ресурса (чаще всего это интернет-магазины, интернет-казино и бизнес или организация, предоставляющие онлайн-услуги). Наиболее крупной атакой с использованием данного инструмента стала DDoS-атак Amazon в июне 2020 года, которая достигла пика в 2,3 Тбит / с.;

– шифрование данных, которое в основном происходит при установке на компьютер программы-вымогателя (чаще всего через сеть интернет при введении жертвы в заблуждение методами социальной инженерии). Данные программы (наиболее популярные CryptoLocker, CryptoWall, Locky и TeslaCrypt) блокируют доступ пользователей к их устройствам или блокируют доступ к файлам до тех пор, пока не будет выплачена денежная сумма или выкуп. Чаще всего, помимо отдельных граждан и частных компаний, атаки направлены на государственный сектор, здравоохранение и обрабатывающую промышленность. Помимо непосредственной блокировки данных, новые версии программ-вымогателей в 2020 году также похищали данные. Самой крупной атакой с использованием данного инструмента в прошедшем (2020) году стало нападение на датскую фирму ISS World – ущерб оценивается от 75 до 112,4 млн долларов. Программы-вымогатели сегодня являются достаточно успешной моделью преступного бизнеса. Например, CryptoWall принесла более 320 миллионов долларов дохода преступникам [6];

– киберфизические атаки представляют собой взлом электрических сетей, транспортных систем, водоочистных сооружений и т. д. Атаки главным образом направлены на критически важную инфраструктуру. Самым громким инцидентом использования подобного инструмента можно назвать атаку на национальную электросеть Украины в 2015 и 2016 годах, в результате чего свыше 200 000 жителей, государственные и частные предприятия остались без электричества [7];

– атаки на IoT (Интернет вещей) – это заражение устройства, подключенного к интернету. Данные атаки в последнее время в ряде случаев используется в совокупности с DDoS-атаками, т. е. злоумышленники получают контроль над устройствами и используют их в качестве элемента распределенной атаки. Только на 2020 год приходилось 12 миллиардов подключений Интернета вещей, что сделало данную область особо привлекательной для злоумышленников [8];

– киберпропаганда (дезинформация) и хактивизм (форма политической активности, при которой навыки компьютерного взлома широко используются против влиятельных коммерческих институтов и правительств, других целей). Ложные новости или киберпропаганда возникли на фоне снижения доверия людей к традиционным СМИ.

Существующие и вновь возникающие угрозы кибербезопасности сегодня направлены на все структуры, имеющие выход в сеть Интернет: частные и государственные организации, производства, медицинские и образовательные учреждения, учреждения здравоохранения, финансовые и банковские структуры, а также многое другое.

2020 год стал одним из наиболее тяжелых периодов для экономики как на национальном, так и мировом уровнях. Усложнившиеся санитарно-эпидемиологические условия позволили злоумышленникам использовать более изощренные средства похищения данных. Так, киберпреступность выросла на 600 % из-за пандемии COVID-19.

Наиболее важными проблемами в данной связи стали:

– интерес пользователей сети Интернет к медицинским и фармакологическим данным делает их мишенью для киберугроз. В 2020 году Google ежемесячно блокировал около 18 миллионов вредоносных и фишинговых писем, связанных с коронавирусом [9];

– сотрудники, работающие в удаленном режиме, являются основной мишенью для киберпреступников. Удаленная работа увеличила среднюю стоимость утечки данных на 137 000 долларов [10].

– основной негативный аспект удаленной работы – увеличение количества утечек через различные сервисы. Полмиллиона учетных записей пользователей Zoom были скомпрометированы и проданы на черном рынке только в апреле 2020 года [11]. Также пандемия Covid-19 заставила многие компании перейти на облачные решения, которые стали новой формой уязвимости компаний;

– отсутствие необходимых навыков кибербезопасности активно влияет на ситуацию с киберпреступностью;

– в результате увеличения пропускной способности устройства, подключенных к Интернету вещей, стали более уязвимыми для кибератак. Многие устройства IoT не разработаны с учетом требований безопасности и могут иметь недостатки и уязвимости, которые легко использовать злоумышленникам. Если хакеры могут получить контроль над устройствами IoT в организации, они потенциально могут использовать их для доступа к остальной части ИТ-системы.

При рассмотрении Республики Беларусь в контексте кибербезопасности, можно утверждать, что проблемы внешнего мира (санитарно-эпидемиологические условия, незащищенность устройств IoT, недостаточная грамотность населения и специалистов в вопросах информационной безопасности и т. п.) также коснулись национального состояния дел. В рейтинге компании Comparitech (2020 год) Беларусь вошла в 10 государств с низким уровнем кибербезопасности (наиболее проблемный аспект – финансовые вредоносные атаки) [12]. В рейтинге Международного союза электросвязи (2018 год) государство заняло 69-ю строчку из 175 возможных по уровню кибербезопасности (падение на 30 пунктов) [13]. Данные показатели демонстрируют необходимость ускорения развития

области кибербезопасности в Республике Беларусь в соответствии с мировыми трендами и угрозами безопасности.

Таблица 1

Статистика киберугроз за февраль 2021 года по данным «Лаборатория Касперского»

OAS / поток данных по вредоносным программам, обнаруженным во время открытия, копирования, запуска или сохранения файлов			MAV / поток данных по вредоносным программам, обнаруженным среди новых объектов в почтовых приложениях		
1	Афганистан	26.49 %	1	Монако	5.77 %
2	Бенин	22.84 %	2	Сербия	5.19 %
3	Буркина-Фасо	22.84 %	3	Монтенегро	4.88 %
4	Таджикистан	22.42 %	4	Южная Африка	4.66 %
5	Эфиопия	22.33 %	5	Хорватия	4.61 %
BAD / статистика по выявленным IP-адресам жертв DDoS-атак и IP-адресам командных серверов ботнетов			RMW / поток обнаружения программ-вымогателей		
1	Китай	13560%	1	Афганистан	2.83 %
2	США	10612%	2	Папуа – Новая Гвинея	1.72 %
3	Россия	1323%	3	Пакистан	1.62 %
4	Великобритания	828%	4	Бангладеш	1.22 %
5	Канада	809%	5	Иран	1.2 %
WAV / поток данных по вредоносным программам, обнаруженным при открытии HTML-страниц веб-сайтов, а также при загрузке файлов			IDS / поток данных по обнаруженным сетевым атакам		
1	Беларусь	25.78 %	1	Эфиопия	22.81 %
2	Алжир	25.34 %	2	Судан	20.39 %
3	Украина	24.24 %	3	Суринам	17.43 %
4	Филиппины	23.26 %	4	Мадагаскар	16.84 %
5	Молдова	23.01 %	5	Иран	16.8 %

На текущий момент в качестве основных координат развития области кибербезопасности принято считать:

– связь инноваций с национальной безопасностью. Развитие области кибербезопасности должно базироваться на создании и внедрении новых технологий безопасности, а также повышении качества образовательных программ. Политика Китая, например, имеет трехслойный подход: крупные инвестиции в исследовательские и технологические фирмы, траты на создание квалифицированной рабочей силы (часто путем финансирования китайских студентов для обучения в западных университетах) и участие в технологическом шпионаже. Инновационная система США также выступает примером на мировой арене ввиду сочетания сильных исследовательских структур, гибких финансовых систем и быстро развивающейся предпринимательской культуры. Модель инновационной системы США включает три класса участников: исследователей, которые придумывают новые идеи, финансистов, готовых идти на риск и инвестировать в новые компании и технологии, и предпринимателей, которые превращают исследования в продукты. Важна корреляция процессов внедрения новых технологий (например, 5G и Iot) и внедрения соответствующих современных средств защиты, ведь именно внедрение новых технологий формирует новую область опасностей, как, например, недостаточная защита устройств, подключенных к интернету вещей сегодня или уязвимость программных продуктов с использованием искусственного интеллекта и машинного обучения;

– новые структуры и профессии. Аспекты кибербезопасности постепенно выходят за рамки ИТ-решений. Специалисты по кибербезопасности должны знать, как планировать и реализовывать стратегии безопасности, разбираться в юридических и этических вопросах, связанных с информационной безопасностью, конфиденциальностью и цифровыми правами и иметь базовые знания в области безопасности компьютерных систем и сетевых методов. Подобные требования ставят новые вызовы перед сферой образования;

– информационная гигиена и цифровая грамотность. Так как большинство атак все еще направлены на человека как на более уязвимый компонент информационной безопасности, становятся необходимыми меры по проведению просветительских и обучающих мероприятиях о работе с информацией из сети Интернет. Учитывая то, что социальная инженерия постоянно развивается и нацелена на злободневные темы (например, как COVID-19) данные мероприятия должны проводиться на постоянной основе. Помимо этого, цифровая грамотность позволяет людям получить необходимые знания об аутентификации, работе с электронными платежами, использовании сетевых подключений и многому другому.

Вопросы кибербезопасности сегодня должны присутствовать во всех видах деятельности, связанных с цифровыми технологиями. Своевременные технологические и организационные решения позволяют уберечь пользователей сети Интернет как физических, так и юридических лиц, от деятельности злоумышленников.

Список литературы

1. Official web-site of Internet World Stats [Electronic resource] // World Internet Users and 2021 Population Stats. [website]. URL: https://www.internetworldstats.com/stats.htm. – Date of access : 06.04.2021.

2. Удальцова Н. Цифровизация экономических процессов в контексте промышленной революции 4.0 / Н. Удальцова. – Режим доступа : https://www.researchgate.net/publication/331462436_Cifrovizacia_ekonomiceskih_processov_v_kontekste_promyslennoj_revolucii_40. – Дата доступа : 08.04.2021.

3. Zacks Investment Researc Macrotrends LLC [Electronic resource] // Yandex Market Cap 2011–2020 [website]. URL: https://www.macrotrends.net/stocks/charts/YNDX/yandex/ market-cap. – Date of access : 07.04.2021.

4. Forbes Media LLC [Электронный ресурс] // Рейтинг Forbes [сайт]. URL: https://www.forbes.ru/biznes-photogallery/421235-30-samyh-dorogih-kompaniy-runeta-reyting-forbes. – Дата доступа : 08.04.2021.

5. Официальный сайт АО «Лаборатория Касперского» [Электронный ресурс] // Статистика кибергугроз [сайт]. URL: https://cybermap.kaspersky.com/ru/subsystems. – Дата доступа : 08.04.2021.

6. The Channel Company [Electronic resource] // The 11 Biggest Ransomware Attacks Of 2020 [website]. URL: https://www.crn.com/slide-shows/security/the-11-biggest-ransomware-attacks-of-2020-so-far-/11. – Date of access : 08.04.2021.

7. Sullivan, Julia & Kamensky, Dmitriy. (2017). How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. The Electricity Journal. 30. 30-35. 10.1016/j.tej.2017.02.006.

8. IoT Analytics GmbH [Electronic resource] // State of the IoT 2020 [website]. URL: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/ (date of access: 08.04.2021).

9. Kumaran N., Lugani S. Protecting businesses against cyber threats during COVID-19 and beyond [Electronic resource] // IDENTITY & SECURITY [website]. URL: https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during covid-19-and-beyond. – Date of access : 08.04.2021.

10. IBM [Electronic resource] // How much would a data breach cost your business? [website]. URL: https://www.ibm.com/security/data-breach. – Date of access : 08.04.2021.

11. Rezonen Pte. Ltd. [Electronic resource] // Half a Million Zoom Accounts Compromised by Credential Stuffing, Sold on Dark Web [online journal]. URL: https://www.cpomagazine.com/cyber-security/half-a-million-zoom-accounts-compromised-by-credential-stuffing-sold-on-dark-web/. – Date of access : 08.04.2021.

12. Comparitech Limited [Electronic resource] // Cybersecurity rating [website]. URL: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/. – Date of access : 08.04.2021.

13. e-Governance Academy Foundation [Electronic resource] // National Cyber Security Index [Electronic resource] URL: https://ncsi.ega.ee/country/by/305/#details. – Date of access : 09.04.2021.

УДК 004.056.53

ПЕРСПЕКТИВЫ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ СОЮЗНОГО ГОСУДАРСТВА

Ю.К. ЯЗОВ, И.С. ГЕФНЕР, С.В. СОЛОВЬЕВ
Федеральная служба по техническому и экспортному контролю,
г. Москва, Российская Федерация
Федеральное автономное учреждение «Государственный научно-исследовательский институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю»,
г. Воронеж, Российская Федерация

Деятельность по защите информации (ЗИ) в информационных системах (ИС) Беларуси и России сегодня связана с решением широкого круга задач, в том числе:

– исследования ИС на предмет определения их классов (уровней) защищенности, выявления источников угроз, уязвимостей в архитектуре, системном и прикладном программном обеспечении, конфигурации (настройках), технологии обработки и передачи информации и др.;

– выявления и оценки рисков реализации возможных угроз безопасности информации;

– обоснования требований по ЗИ и формирования адекватных решений по защите с оценкой их эффективности и выбором приемлемых мер и средств, позволяющих выполнить обоснованные требования;

– определения целесообразных путей построения и создании систем защиты информации в составе ИС;

– организации и обеспечения выполнения мероприятий по ЗИ;

– разработки необходимых организационно-распорядительных и методических документов по ЗИ;

– организации и проведения контроля и оценка защищенности информации, обрабатываемой в ИС, выявление основных проблем в области ЗИ и выработка предложений по их решению и др.

Состав и содержание этих задач обусловлены содержанием предметной области ЗИ (рис. 1), при этом качество их решения во многом определяется полнотой, своевременностью предоставления и достоверностью информации, необходимой для организации и ведения ЗИ в ИС [1]. Однако сегодня имеет место целый ряд факторов, существенно осложняющих обеспечение такой информацией. К ним относится большое разнообразие характеристик ИС (состава применяемого оборудования и программного обеспечения, топологий построения, технологий обработки информации и т. д.), существенных для ЗИ условий их функционирования, ну и, конечно, постоянно расширяющийся спектр угроз и способов их реализации, огромное разнообразие решений, которые приходится обосновывать при организации и ведении ЗИ. Уже неоднократно на предыдущих конференциях поднимался важный вопрос анализа и оценки нового класса угроз безопасности информации, реализуемых с использованием уязвимостей аппаратной платформы, то есть через чипсет, а сегодня вероятности реализации таких угроз существенно возросли. Вместе с тем, сведения о них сегодня практически не учитывается при организации защиты. Наконец, быстро разрастаются объемы информации, касающейся требований нормативных документов по ЗИ, которых в России насчитывается уже несколько сотен.

Все это вынуждает автоматизировать процессы информационного обеспечения (ИО) деятельности по ЗИ, создавать в рамках ИС специальные в информационных системахподсистемы ИО деятельности по ЗИ (далее системы информационного обеспечения – СИО).

Такие СИО, по сути, являются системами поддержки принятия решений, предназначенными, во-первых, для выбора и своевременного предоставления заинтересованным лицам

информации, необходимой при решении задач ЗИ, а также для сбора, систематизации и хранения такой информации, поддержки ее в актуальном состоянии, во-вторых, для обеспечения проведения расчетов, необходимых при обосновании выбора мер и средств защиты, и предоставления по запросу результатов таких расчетов и обоснований, в-третьих, для сбора, систематизации, актуализации и предоставления информации, полученной по результатам контроля защищенности информации в ИС, в четвертых, для формирования, хранения и предоставления вариантов построения систем защиты информации в ИС Союзного государства, предоставления примеров содержания отрабатываемых документов по организации ЗИ и др.

Важным факторов развития СИО является появление новых информационных технологий ЗИ в ИС, которые сегодня или только начинают разрабатываться, или уже внедряются в практику. Речь идет о технологиях искусственного интеллекта, в том числе: машинного обучения, нейронных сетей, методов и алгоритмов эволюционного моделирования (генетических алгоритмов), а также о технологии многоагентных систем ЗИ. Соответственно должно меняться и ИО реализации таких технологий защиты.

Сегодня не только исследуются и разрабатываются новые подходы, направленные на совершенствование ИО, но и начинают внедряться, например, картографические методы кластеризации сведений и их источников при автоматизированном поиске информации в Internet в ходе решения задач прогнозирования угроз безопасности информации, поиска сведений о новых уязвимостях и эксплойтах [2], методы теории нечетких множеств и нечеткой логики при формировании решений при анализе угроз безопасности, при оценке возможностей и последствий реализации угроз и др.

Все это обусловливает формирование нового облика перспективных СИО, которые целесообразно иметь для решения задач ИО деятельности по защите информации в ИС Беларуси и России (рис. 2).

Вместе с тем следует отметить, что решения по рациональному построению СИО должны приниматься на основе, во-первых, прогнозных оценок эффективности возможных вариантов такого построения в ходе проектирования, во-вторых, оценок эффективности функционирования СИО в ходе организации и ведения ЗИ, когда реализуются функции «сбора, контроля, преобразования, хранения, обновления, распределения и передачи информации» [3]. Наконец, динамично изменяющиеся условия организации и ведения ЗИ (изменения нормативной базы, появление новых угроз безопасности информации и уязвимостей системного и прикладного программного обеспечения, совершенствование средств и систем защиты информации и т. д.) обусловливает необходимость регулярного расширения используемого информационного пространства, создания саморегулирующейся СИО, способной гибко и оперативно перестраивать свое функционирования и осуществлять наращивание возможностей по информационной поддержке проводимых мероприятий по ЗИ, то есть фактически необходимо прогнозировать изменение предметной области ЗИ информации.

Однако методическое обеспечение ни для оценки эффективности информационного обеспечения деятельности по ЗИ, ни для прогнозирования изменений предметной области ЗИ до сих пор не разрабатывалось.

При этом под эффективностью здесь понимается степень соответствия предоставляемых услуг в ИО потребностям организации ЗИ в ИС. В таком понимании эффективность ИО является функцией показателей, характеризующих, прежде всего, полноту, достоверность, своевременность (актуальность) и защищенность предоставляемой информации, необходимой для организации в ЗИ в ИС органа власти, предприятия, организации.

На наш взгляд, в состав такого обеспечения необходимо включить комплекс моделей и методик, которые позволили бы принимать обоснованные решения как по рациональному построению СИО в ИС, так и в интересах качественного и своевременного выполнения мероприятий по ЗИ. Вариант состава моделей и методик, необходимых для создания и эксплуатации СИО деятельности по ЗИ применительно к различным стадиям жизненного цикла этой системы, приведен на рис. 3.

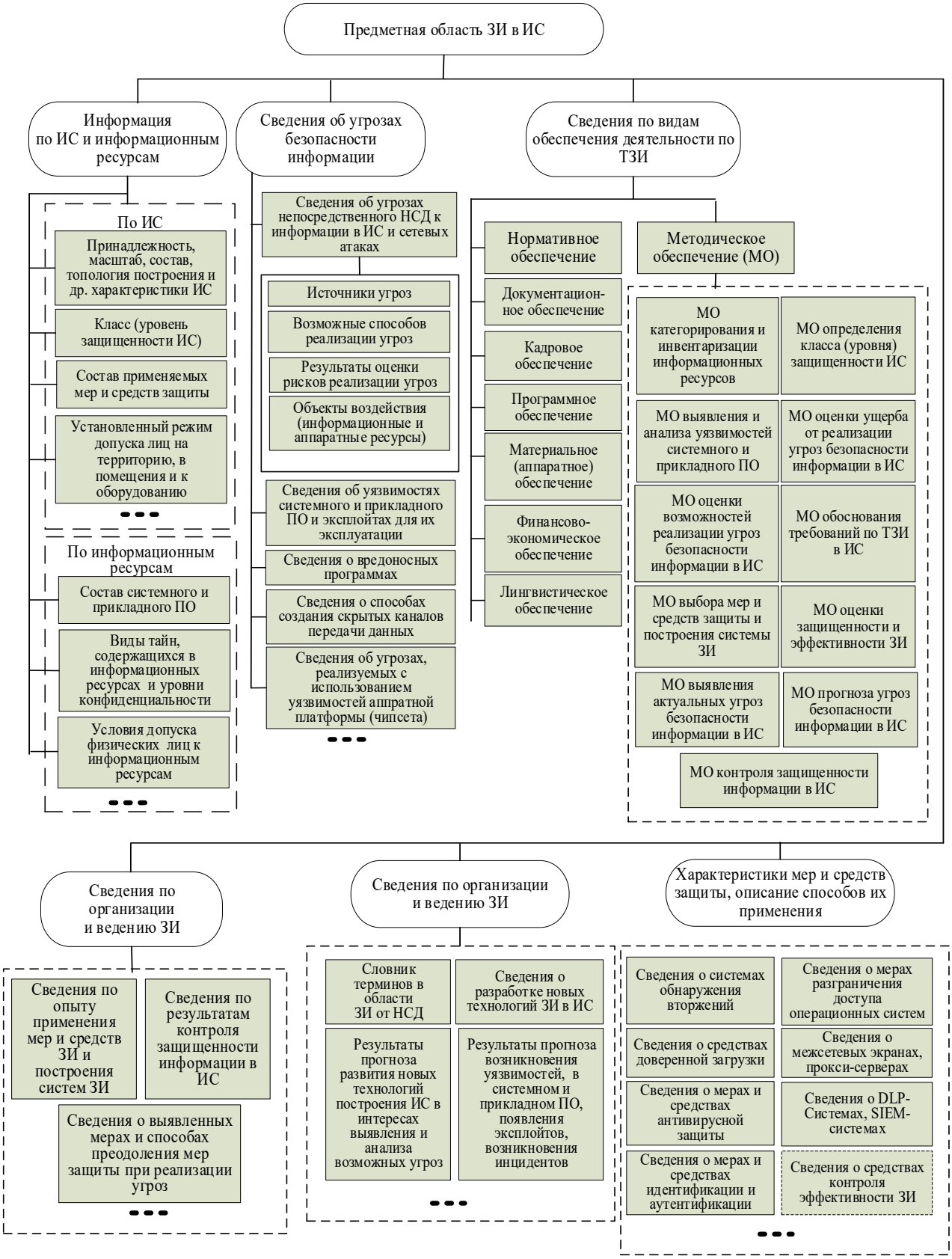


Рис. 1. Структура предметной области защиты информации от несанкционированного доступа

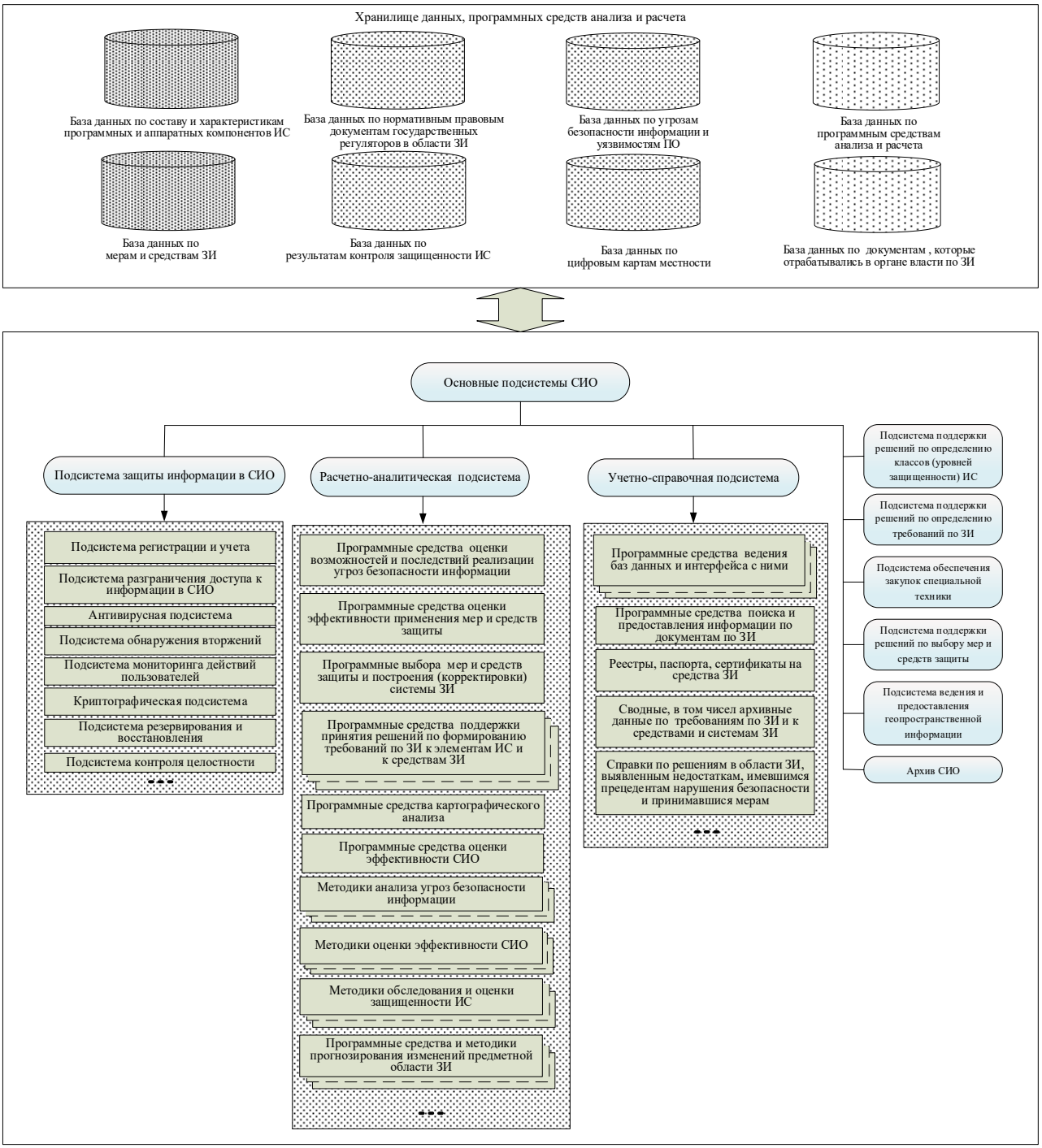


Рис. 2. Состав и структура системы информационного обеспечения деятельности по организации и ведению защиты информации в информационных системах (вариант)

Таким образом, для автоматизации процессов ИО деятельности по ТЗИ в ИС Беларуси и России необходимо иметь автоматизированные СИО, для создания и функционирования которых требуется разработка соответствующего методического обеспечения. Предложенный состав и структура системы моделей и методик позволит обеспечить решение задач обоснования требований к СИО, создания таких систем и тем самым повысить эффективность ИО деятельности по ЗИ с учетом динамично меняющейся предметной области ЗИ, интенсивного развития информационных технологий и регулярного изменения нормативной базы по ЗИ.

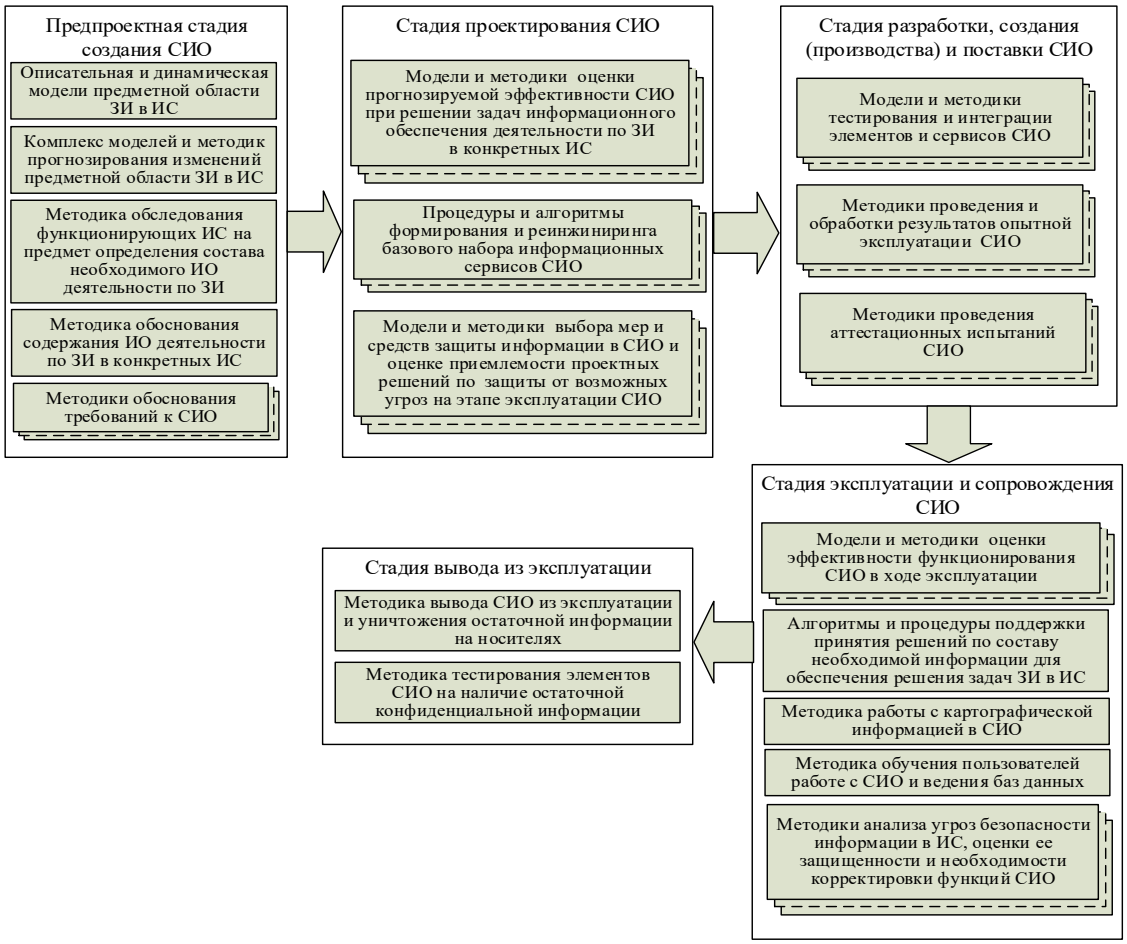


Рис. 3. Вариант состава методического обеспечения, необходимого для создания и эксплуатации СИО, деятельности по ЗИ применительно к различным стадиям жизненного цикла этой системы

Список литературы

1. Язов, Ю. К. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю. К. Язов, С. В. Соловьев. – Воронеж : Кварта, 2018. – 588 с.

2. Serdechnyi, A. L. MAPPING RETRIEVAL METHOD FOR ACADEMIC PUBLICATIONS IN THE FIELD OF AEROSPACE TECHNOLOGY SAFETY / A. L. Serdechnyi [et al.] // IOP Conference Series : Materials Science and Engineering. Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations, 2020. – P. 520–528.

3. Сюнтюренко, О. В. Информационное обеспечение: факторы развития, управление, эффективность / О. В. Сюнтюренко // Научно-техническая информация. Серия 2: Информационные процессы и системы. – 2016. – № 6. – С. 7–15.

УДК 007.51

ОСНОВНЫЕ НАПРАВЛЕНИЯ СОЗДАНИЯ И РАЗВИТИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ СОЮЗНОГО ГОСУДАРСТВА

С.В. ЖЕРНОСЕК, Р.Ф. НАРДИНОВ
Оперативно-аналитический центр при Президенте Республики Беларусь,
г. Минск, 220030, Республика Беларусь

Современный мир бросает новые вызовы и угрозы национальной безопасности. Сегодня воздействие на информационно-коммуникационную инфраструктуру, информационные системы и ресурсы является одним из инструментов давления на государство.

Создание и функционирование комплексной системы защиты информации в информационных системах, способной адекватно реагировать на новые угрозы информационной безопасности, становится одним из важных факторов, которые обеспечивают социально-экономическое развитие государств.

Целями стартовавшей в 2000 году программы Союзного государства «Защита общих информационных ресурсов Беларуси и России» (2000–2004 годы) являлось объединение потенциалов и ресурсов России и Беларуси для повышения эффективности национальных систем защиты информации, а также обеспечение реализации первоочередных задач Союзного государства, в том числе, таких как обеспечение функционирования взаимоувязанных систем связи и телекоммуникаций, формирование и обеспечение безопасности единого информационного пространства.

Так, в рамках программы разработаны:

– Концепция обеспечения безопасности информационных и телекоммуникационных технологий;

– перечень совместно используемых информационных ресурсов и информационно-коммуникационной инфраструктуры, подлежащих защите, и положение о системе защиты совместных информационных ресурсов Союзного государства;

– требования к технологиям контроля создания программных продуктов и автоматизированных систем, отвечающих требованиям по защите информации;

– проекты технических нормативных правовых актов и единых образовательных стандартов и многие другие документы, которые позволили обеспечить решение задач по гармонизации национальных законодательств в области защиты информации, государственному контролю за разработкой, сертификацией, применением средств защиты информации [1].

Создание и динамичное развитие критически важных систем информационной инфраструктуры, и, как следствие, необходимость выработки научно-технических решений для реализации мер по предупреждению и нейтрализации угроз безопасности информации этих систем, определило основное направление новой программы Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий» на 2006–2010 годы.

Основные направления научных исследований и разработок в рамках программы:

– разработка нормативно-технических документов (в том числе технических нормативных правовых актов) по обеспечению безопасности информации на критически важных объектах;

– создание и развитие информационно-технической системы контроля безопасности информации на критически важных объектах, а также защиты совместных информационных ресурсов Союзного государства;

– перспективные технологии защиты совместных информационных ресурсов Союзного государства от утечки и воздействия по техническим каналам, несанкционированного доступа, от компьютерных атак и вирусов.

По результатам выполнения программы 2006–2010 годов завершен процесс формирования нормативной базы обеспечения защиты информации в инфраструктуре Союзного государства [2]. С учетом развития межгосударственного электронного взаимодействия одним

из направлений разработок в период 2011–2015 годы стало формирование и обеспечение функционирования трансграничного пространства доверия. Так в рамках программы «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий» на 2011–2015 годы разработаны технические нормативные правовые акты и комплексы программно-аппаратных средств инфраструктуры открытых ключей, позволяющих предоставлять доверенные сервисы для межгосударственного обмена электронными документами [3]. В указанный период также был разработан ряд средств технической и криптографической защиты информации.

Таким образом, программы 2000–2015 годов обеспечили принятие эффективных мер по предупреждению и нейтрализации угроз безопасности информации в информационных системах, в том числе на критически важных объектах.

Необходимо также отметить, что усиление информационной безопасности Союзного государства в сфере защиты информационных ресурсов в информационных системах также отнесено к приоритетным направлениям развития Союзного государства на 2018–2022 годы.

Решение задач противодействия новым вызовам и угрозам в информационной сфере в настоящее время осуществляется посредством реализации мероприятий программы Союзного государства в указанный период [4].

Так, по результатам уже выполненных мероприятий программы:

– разработаны технические требования на создание информационной системы региональных и национального центров выявления и противодействия угрозам и инцидентам информационной безопасности;

– разработано программно-аппаратное средство обеспечения IP-коммуникаций на мобильных устройствах, которое применяется для решения задач по обеспечению мероприятий с участием лиц, входящих в состав Высшего Государственного Совета Союзного государства.

Поступательное развитие и своевременное принятие мер по защите информации и информационных ресурсов Союзного государства и государств-участников является одним из важных факторов, влияющих на развитие Союзного государства. Государственными заказчиками программы проводится работа по формированию проекта Концепции соответствующей программы Союзного государства на 2023–2027 годы. К основным направлениям развития системы защиты информации в информационных системах Союзного государства в ближайшей перспективе следует отнести создание информационной системы региональных и национального центров выявления и противодействия угрозам и инцидентам информационной безопасности, обеспечение мер технической и криптографической защиты персональных данных.

Список литературы

1. Об итогах выполнения программы Союзного государства «Защита общих информационных ресурсов Беларуси и России : Пост. Совета Министров Союзного государства, 29 окт. 2005 г., № 25.

2. Об итогах выполнения программы Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на 2006–2010 годы» : Пост. Совета Министров Союзного государства, 22 апр.я 2011 г., № 6.

3. Об итогах выполнения программы Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на 2011–2015 годы» : Пост. Совета Министров Союзного государства, 16 июня 2017 г., № 23.

4. О выполнении приоритетных направлений и первоочередных задач дальнейшего развития Союзного государства на среднесрочную перспективу (2014–2017 гг.) и дальнейшем развитии Союзного государства на 2018–2022 гг. : Пост. Высшего Гос. Совета Союзного государства, 19 июня 2018 г., № 3.

УДК 004.056

ОБ УГРОЗАХ, МЕРАХ ЗАЩИТЫ И ПРОТИВОДЕЙСТВИЯ ОТ ДЕСТРУКТИВНОГО ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ НА ГРАЖДАНСКОЕ ОБЩЕСТВО СОЮЗНОГО ГОСУДАРСТВА

А.И. ЧИСЛОВ
Тюменский институт повышения квалификации,
г. Тюмень, Российская Федерация

Обеспечение национальной безопасности является для развития всех стран центральной стратегически значимой задачей. Масштабные социально-коммуникационные трансформации оказывают не только позитивное влияние на развитие общества, но и неизбежно государство сталкивается с негативными дезогранизирующими нормальное функционирование различных институтов государства и общества явлениями, прежде всего информационные угрозы. Особое внимание уделяется угрозам деструктивного информационного воздействия на гражданское общество, которые стали нередки в современном мире и, к сожалению, происходят как в России, так и в Белоруссии, в частности так называемые марши несогласных и «карнавальные шествия».

Как справедливо отмечает доктор исторических наук, процессор Леонид Владимирович Карнаушенко условия постиндустриального информационного пространства, особенно потенциал воздействия информационно-компьютерных технологий на сознание и поведение людей, требуют эффективного, прежде всего практически ориентированного научного анализа. Особое внимание следует обратить на риски и угрозы деструктивного влияния агрессивных коммуникаторов на сознание и, соответственно, поведение массовой аудитории посредством информационно-компьютерных и телекоммуникационных технологий.

Законодательство Российской Федерации несколько последних лет направлено на выработку мер правового и организационного характера, направленных на защиту гражданского общества от деструктивного информационного воздействия. 5 декабря 2016 г. вступил в силу Указ Президента Российской Федерации № 646, утвердивший новую Доктрину информационной безопасности, которая стала существенным шагом, направленным на регулирование вопросов информационной безопасности в нашей стране. Прежде всего, было дано понятие информационной безопасности, под которой понимается состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие России, оборона и безопасность государства. При этом под угрозой информационной безопасности понимается совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.

Состояние информационной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры. По данным Совета Безопасности РФ, в 2016 году было зафиксировано около 52,5 млн кибератак на веб-сайты госорганов (в 2015 году – 14,4 млн). Цель большинства атак – получение информации ограниченного доступа и нарушение функционирования технических средств (по данным Интерфакс от 03.03.2017).

Для минимизации масштабов киберугроз в Российской Федерации был принят Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который устанавливает организационно-правовые основы обеспечения безопасности критической инфраструктуры в целях ее устойчивого функционирования, определяет права и обязанности ее владельцев, а также полномочия госорганов в указанной сфере. Под безопасностью критической информационной инфраструктуры (КИИ) понимается состояние защищенности критической информационной инфра-

структуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак.

В организационном плане для решения проблем обеспечения информационной безопасности требуются соответствующие управленческие кадры, специалисты-профессионалы в этой актуальной сфере человеческой деятельности работу которых необходимо строить на анализе формирования и развития постиндустриального общества.

Современную социальную систему, по мысли канадского социолога М. Маклюэна, следует признать инновационной формой социальной организации, поскольку она обладает атрибутивными характеристиками, позволяющими возрождать естественное слуховизуальное многомерное восприятие мира и коллективность, используя при этом современную электронную, информационно-коммуникационную основу, где традиционные письменно-печатные языки общения замещаются радиотелевизионными и сетевыми средствами массовых коммуникаций. В свою очередь испанский социолог М. Кастельс обосновал концепцию общества сетевых структур, в котором ведущую роль играют информационно-компьютерные технологии, создающие особую интернет-среду и, таким образом, воздействующие на генезис новой формы социальной и социокультурной реальности. С этой точки зрения интернет-коммуникация выходит значительно дальше пределов собственно средства массовой коммуникации, интенсивно воздействуя на социальную структуру, социальные процессы и институты.

Преимущества новой высокотехнологичной среды, в большей части агрессивные факторы стремятся использовать преступные элементы для получения тактического преимущества над правоохранительной системой государства, что обусловлено объективными факторами из-за существенной инерционности норм права.

Стоит отметить, что с развитием технологического общества активизируются террористы, экстремисты, радикалы, киберпреступники и другие, которые умело пользуются, не скупясь на затратную часть, проводят планомерное манипуляционное воздействие на сознание членов гражданского общества с целью формирования деструктивного духовно-нравственного противозаконного поведения.

Информационное воздействие осуществляется в различных формах, однако чаще всего в форме манипуляции сознанием. Этот вид массово-коммуникативного воздействия является одним из наиболее опасных в современном высокотехнологичном мире. Отсутствие своего рода тотального контроля, или даже как, например, в государстве Сингапур цензуры интернета, социальных сетей и т. п., а также своевременного реагирования на законодательном уровне по введению ответственности. В научной литературе представлено множество фундаментальных трудов, посвященных проблеме манипуляции сознанием. По мнению Л.В. Карнаушенко манипуляция сознанием в ходе массово-коммуникативного воздействия направлена на установление и поддержание контроля над сознанием и поведением значительных по численности социальных групп, общностей или всего социума в целом. Такого рода влияние особенно опасно в современном высокотехнологичном социуме, т. к. его инструментами выступают аудиовизуальные массмедиа и глобальная сеть Интернет, которые имеют широкие возможности воздействия на массовую аудиторию. Именно так агрессивный коммуникатор, находясь на расстоянии от управляемой массовой аудитории (в том числе и за пределами национальных границ государства), обладает широким возможностями управления ее сознанием, а, следовательно, в значительной мере – и ее поведением, изменяя ее мнения, идеалы, картины мира, потребности и т. д. В необходимом для организатора (или организаторов) направлении.

В свое время в 2006 г. И.Н. Панарин в работе «Информационная война и геополитика» обозначил, что сейчас происходит пятая мировая война – информационно-интеллектуальная, она ведется не только на политическом и финансовом, но и на культурном, цивилизованном, этническом, религиозном и иных фронтах. И как показывает история, во всех войнах вспомогательным средством служит ослабление духа вражеской армии и народа. Активное использование коллаборационистов, подрыв духовной целостности врага и сохранение от разложения собственного духа.

При этом следует отметить, что средства информационного воздействия классифицируют по характеру поражающих свойств:

– высокоточное воздействие (на определенных лиц, на избранный социальный срез общества, на определенный ресурс в информационно-вычислительной сети);

– комплексное воздействие (все население некоторого региона, а также вся его информационно-телекоммуникационная инфраструктура).

Тип информационного воздействия может быть:

а) разрушающим;

б) манипулирующим;

в) блокирующим.

С.И. Макаренко в своей монографии «Информационное противоборство и радио–электронная борьба в сетецентрических войнах начала XXI века» классифицирует технологии информационного противоборства, обеспечивающего разработку и применение информационного оружия.

Стоит обратить внимание на то, что Доктрина информационной безопасности Российской Федерации акцентирует внимание на том, что «реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина». Совершенно очевидно, что именно обеспечение качественной информацией населения нашей страны способно защитить от множества угроз и вызовов, в том числе скрытого манипулятивного воздействия на сознание людей.

В нашей стране с достаточно серьезным опозданием законодатель обратил внимание, что наряду с безопасностью информационных систем, информационной инфраструктуры критически важно обеспечивать защиту психики, личности, менталитета, системы ценностей, морально-нравственных принципов людей от агрессивной, вредоносной информации, т. К., например, панические слухи, домыслы, дезинформация могут стать причиной масштабных социальных конфликтов, дезорганизации социальной системы. В настоящее время возникший дисбаланс в целом преодолевается. Однако все же следует учитывать, что решение проблемы – это не только декларации, но и сложная система органически связанных между собой нормативных правовых актов. В данном аспекте еще необходимо повышать эффективность государственной власти, прежде всего, в аспекте экспертизы принимаемых нормативных правовых актов. Необходимо отметить, что в Доктрине вполне закономерно в числе стратегических целей и основных направлений обеспечения информационной безопасности указывается и «нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества».

Очевидно, что угрозы информационного деструктивного воздействия на гражданское общество приобретают свои очертания, и законодатель находится в процессе выработки механизма противодействия этим угрозам. В настоящее время от успешного взаимодействия политического, технологического, в том числе и IT компаний, а также с участием представителей гражданского общества. Примером служит Перечень поручений по итогам заседания Совета по развитию гражданского общества и правам человека от 10 декабря 2020 года, в котором В.В. Путин поручил:

1. Администрации Президента Российской Федерации подготовить совместно с Правительством Российской Федерации и представить предложения по установлению дополнительных требований к зарубежным технологическим компаниям, осуществляющим деятельность в российском сегменте информационно-телекоммуникационной сети Интернет, в том числе в части, касающейся открытия представительств этих компаний на территории Российской Федерации.

2. Полномочным представителям Президента Российской Федерации в федеральных округах совместно с Советом при Президенте Российской Федерации по развитию гражданского общества и правам человека принять меры по обеспечению в субъектах Российской Федерации прав журналистов, предусмотренных законодательством Российской Федерации о средствах массовой информации.

3. Правительству Российской Федерации:

г) совместно с Советом при Президенте Российской Федерации по развитию гражданского общества и правам человека разработать проект концепции обеспечения защиты прав и свобод человека и гражданина в цифровом пространстве Российской Федерации и проект плана мероприятий («дорожной карты») по ее реализации, включающего в себя мероприятия по повышению цифровой грамотности граждан Российской Федерации и их обучению навыкам информационной безопасности и «цифровой гигиены».

8. Рекомендовать Верховному Суду Российской Федерации:

а) с учетом ранее данных поручений подготовить разъяснения по итогам обобщения судебной практики по делам, связанным с нарушениями законодательства о свободе совести, свободе вероисповедания и религиозных объединениях;

б) проанализировать совместно с Генеральной прокуратурой Российской Федерации практику применения статьи 280 Уголовного кодекса Российской Федерации («Публичные призывы к осуществлению экстремистской деятельности») и рассмотреть вопрос о возможности введения административной преюдиции по указанной статье;

в) рассмотреть совместно с Министерством юстиции Российской Федерации вопрос о целесообразности создания российского суда по правам человека и представить при необходимости соответствующие предложения.

Таким образом, несмотря на принимаемые в Российской Федерации по противодействию угрозам деструктивного информационного воздействия на гражданское общество, следует отметить что они являются недостаточными как в правовом, так и в организационном плане. Прежде всего необходима консолидация усилий не только внутри своего государства, но и в межгосударственном взаимодействии Союзного государства. Назрела необходимость принятия соответствующего международного документа, в котором необходимо обозначить основные принципы формирования информационного пространства, инструменты воздействия на порядок его формирования, формы профилактического воздействия на попытки деструктивного информационного воздействия, а также меры по пресечению таких угроз.

УДК 004.056

АКТУАЛЬНЫЕ ВОПРОСЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

С.В. КУТУЗОВ
Оперативно-аналитический центр при Президенте Республики Беларусь

Нормативные и технические нормативные правовые акты, регулирующие вопросы криптографической защиты информации. Криптографическая защита информации – деятельность, направленная на обеспечение конфиденциальности, контроля целостности и подлинности информации с использованием средств криптографической защиты информации.

Средства криптографической защиты информации – программные, программно-аппаратные средства, реализующие один или несколько криптографических алгоритмов (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита) и криптографические протоколы, а также функции управления криптографическими ключами и функциональные возможности безопасности.

Задачи, решаемые криптографическими методами: обеспечение конфиденциальности, контроль целостности и подлинности, аутентификация, невозможность отказа от авторства.

НПА регулирующие вопросы криптографической защиты информации – Законы Республики Беларусь «Об информации, информатизации и защите информации», «Об электронном документе и электронной цифровой подписи»; Указы Президента Республики Беларусь от 01.09.2010 №450, от 16.04.2013 №196; приказы ОАЦ №66 от 20.02.2020г., №89 от 29.11.2013 г., №118 от 10.12.2015г., №77 от 12.03.2020г.;

ТНПА регулирующие вопросы криптографической защиты информации – технический регламент ТР 2013/027/BY и государственные стандарты Республики Беларусь (СТБ 1176.1,.2, СТБ 34.101.17, .18, .19, .21, .23, .26, .27, .31, .45, .47, .60, .65, .66, .67, .77, .78, .79, .80, .81, .82).

Данные стандарты определяют требования к алгоритмам криптографических преобразований и протоколам (алгоритмам шифрования и режимам его использования – СТБ 34.101.31-2011 и СТБ 34.101.77, процедурам выработки и проверки электронной цифровой подписи – СТБ 1176.2-99, СТБ 34.101.45-2013, функции хэширования – СТБ 1176.1-99, СТБ 34.101.31-2011, СТБ 34.101.77, протоколу TLS – СТБ 34.101.65-2014), управления криптографическими ключами (алгоритмы генерации псевдослучайных чисел – СТБ 34.101.47-2012, формат запроса на издания сертификата открытого ключа – СТБ 34.101.17-2012, формат сертификата открытого ключа и списка отозванных сертификатов – СТБ 34.101.19-2012, алгоритм разделения секрета – СТБ 34.101.60-2014, протоколы формирования общего ключа на основе эллиптических кривых – СТБ 34.101.66-2014 и другие). Определены требования безопасности к программным, программно-аппаратным и техническим средствам криптографической защиты информации – СТБ 34.101.27-2011 и СТБ П 34.101.43-2009. Установлены требования к профилю ИОК СТБ 34.101.78 и службам ИОК СТБ 34.101.67 (атрибутные сертификаты), СТБ 34.101.26 (ocsp), СТБ 34.101.81 (dvcs), СТБ 34.101.82 (tsp). Форматам криптографических данных – СТБ 34.101.23 (CSM), СТБ 34.101.50 (XML Dsig/Enc), СТБ 34.101.80 (AxDES). Также установлены требования к аппаратным криптографическим токенам – СТБ 34.101.79, ID-картам – профиль в СТБ 34.101.79.

Инфраструктура криптографической защиты информации. Государственное регулирование и управление в сфере технической и криптографической защиты информации осуществляются Президентом Республики Беларусь и Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – ОАЦ).

ОАЦ:

– определяет приоритетные направления технической и криптографической защиты информации;

– координирует деятельность государственных органов и иных организаций (далее – организации) по применению мер технической и криптографической защиты информации;

– осуществляет контроль за технической и криптографической защитой информации в организациях;

– определяет порядок: технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено; аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено (далее – аттестация систем защиты информации); технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации, в том числе порядок проведения аудита систем информационной безопасности критически важных объектов информатизации;

– организует и осуществляет техническое нормирование и стандартизацию по вопросам технической и криптографической защиты информации;

– осуществляет: **лицензирование деятельности по технической и (или) криптографической защите информации**; **подтверждение соответствия и проведение государственной экспертизы средств технической и криптографической защиты информации**, за исключением средств шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов, определяет порядок проведения такой экспертизы;

– выносит письменные требования (предписания) об устранении организациями выявленных нарушений настоящего Положения и иных нормативных правовых актов в сфере технической и криптографической защиты информации и (или) приостановлении (прекращении) обработки информации в информационной системе или функционирования критически важного объекта информатизации;

– выступает заказчиком государственных научно-технических и иных программ и проектов, обеспечивает организацию и проведение научно-исследовательских, опытно-конструкторских и иных работ в сфере технической и криптографической защиты информации;

– осуществляет международное сотрудничество в сфере технической и криптографической защиты информации, в том числе взаимодействует с организациями иностранных государств и международными организациями, заключает в пределах своей компетенции международные договоры межведомственного характера;

– разрабатывает проекты актов законодательства, в том числе обязательных для соблюдения технических нормативных правовых актов, и принимает такие акты по вопросам технической и криптографической защиты информации;

– осуществляет иные полномочия в сфере технической и криптографической защиты информации в соответствии с настоящим Положением и иными законодательными актами

Имеют лицензия на осуществление деятельности по технической и (или) криптографической защите информации в части составляющих работ и услуг по разработке и производству средств криптографической защиты информации 29 организаций с различной формой собственности.

38 организаций имеют лицензию на оказание услуг по распространению открытых ключей проверки электронной цифровой подписи (УЦ и РЦ). Из них аккредитованы в ГосСУОК 13 организаций (издано более 960 тысяч сертификатов).

Направления развития инфраструктуры криптографической защиты информации

В части стандартизации – разработка СТБ, устанавливающих требования к протоколам идентификации/аутентификации (топология, процессы, токены аутентификации, протоколы, OAuth/OIDC), облачной подписи (архитектура, требования безопасности), требованиям безопасности аппаратных средств криптографической защиты информации.

В части развития ГосСУОК – переход на новую платформу РУЦ, внедрение сервисов по изданию атрибутных сертификатов, онлайн проверки действительности сертификатов, штампа времени, заверения данных, запуск национального ДТС.

Поддержка трансграничного пространства цифрового доверия в рамках ЕврАзЭС и с другими странами.

Купирование вопросов несовместимости средств криптографической защиты информации, высокой стоимости, юзаби́лити.

Внедрение ID-карты гражданина Республики Беларусь.

УДК 004.056

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ И НОВЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ СОЮЗНОГО ГОСУДАРСТВА

В.Р. ГРИГОРЬЕВ
Институт комплексной безопасности и специального приборостроения, РТУ МИРЭА, г. Москва, Российская Федерация

Введение. Новые тенденции в развитии информационных технологий и их монополизация транснациональными телекоммуникационными компаниями создают новые риски для информационной безопасности Союзного государства. В современном мире информация стала стратегическим ресурсом, от уровня развития национальной информационной инфраструктуры зависит экономический, оборонный и политический потенциал любой развитой страны. При этом возрастает уязвимость этой инфраструктуры к различным негативным воздействиям. Происходят глобальные стратегические вызовы, к числу которых можно отнести, в том числе, и формирующуюся на наших глазах «цифровую экономику», которая быстро становится новым инструментом гибридной войны. Это касается и технологической основы «цифровой экономики» в виде необходимости создания национальной платформы – интегрированной информационной системы Евразийского экономического союза (ИИС ЕЭС). Это и вопросы создания многосвязных распределенных во времени и пространстве сетевых объектов «социо-киберфизические систем». Это и вопросы гармонизации нормативно-правовой базы в области информационной безопасности, принятой в обоих государствах. Это и совместные подходы к процессу подготовки кадров для реализации национальных программ создания в России и Беларуси инфраструктуры цифровой экономики. Все эти актуальные задачи объединяет необходимость разработки Концепции коллективной информационной безопасности Союзного государства. Информационная безопасность становится важнейшей составляющей во всей системе как национальной, так и коллективной безопасности Союзного государства.

1. Технологический уровень вызовов и рисков для обеспечения информационной безопасности социо-киберфизических систем. Новые тенденции в развитии информационных технологий создают новые риски для информационной безопасности любого государства. Цифровой мир стремительно расширяется, он становится мобильным, управляет производством и технологическими процессами, охватывает всю среду обитания человека – от бытовых приборов до умных офисов и интеллектуального транспорта. Все больше информации передается через мобильные сервисы, ранее изолированные системы начинают взаимодействовать и обмениваться информацией, лавинообразно нарастает поток данных и объемы хранения. Внедрение новых парадигм организации распределенных крупномасштабных систем, таких как «Интернет вещей» (Internet of Things, IoT), приведет к новым рискам информационной безопасности, когда через сеть станут доступны практически все предметы, окружающие человека.

По мере развития технологий в окружающем человека мире появляется все больше устройств, находящихся под управлением микропроцессоров и программного обеспечения. С ростом числа внедрений решений на базе IoT, как считают эксперты, все больше атак будет направлено не только на ПО, но и на аппаратное обеспечение (микпроцессоры, сетевые карты, USB устройства), входящее в инфраструктуру «интеллектуального транспорта», «умных домов», автоматизированных систем управления производством.

В связи с этим вопросы обеспечения информационной безопасности таких многосвязных распределенных во времени и пространстве сетевых объектов начинают основываться на понятии «социо-киберфизические системы» – нового (термин Cyber Physical System появился в 2006 году), но очень перспективного инновационного направления. CPS – это системы, состоящие из различных природных объектов, искусственных подсистем и управляющих контроллеров, которые представляют собой единое целое. Добавление «social» подра-

зумевает вовлечение в эту систему человека и общества. Предпосылками появления таких сложных механизмов принято считать освоение наукой и промышленностью различных вычислительных, автоматизированных и сенсорных систем. Отличие CPS состоит в том, что они подразумевают тесное взаимодействие технологий с физическими ресурсами: социо-киберфизические системы основаны на инженерном моделировании и способны адаптироваться к изменениям окружающей среды.

Для поддержки этого нового инновационного направления в ближайшее время будут разработаны алгоритмы машинного обучения и гибкое программное обеспечение, которые помогут упорядочить информацию о физическом мире и организовать масштабный сбор данных с миллиардов устройств в рамках существующего видения и понимания киберфизических систем и искусственного интеллекта. Таким образом, кибер-физическая система (англ. cyber-physical system) представляет собой информационно-технологическую концепцию, которая предполагает интеграцию вычислительных ресурсов в физические процессы.

Интегрированная технология реализации киберфизических систем – Интернет вещей – является инфраструктурой создаваемого информационного общества. Датчики и сенсоры, умный дом и умный город, машины, обменивающиеся информацией друг с другом: чтобы все это, заработало, выход в интернет должен быть доступен повсеместно и в любой момент времени.

Также следует отметить, что, исходя из современных концепций проектирования информационных систем следует, что любая ИС является социотехнической, причем отношения между субъектами в большей или меньшей степени могут быть недостаточно формализованы и, таким образом, иметь характер конфликта.

Социотехническая информационная система (СТИС) – совокупность информационно-технической и социальной инфраструктур ИС. Социотехнической является любая ИС, где социальная инфраструктура, то есть «человеческий фактор», оказывает непосредственное влияние на эффективность использования компьютерной техники. Человеческий фактор также затрагивает стадии функционирования всей ИС, такие как проектирование, разработка, внедрение, эксплуатация. Управляемость социальной среды, профессиональные навыки и квалификация специалистов, а также общее понимание поставленных задач являются важнейшими составляющими ИС и информационных технологий вообще. Представление ИС социотехнической системой предопределяет и подход к анализу ее безопасности.

Обеспечение безопасности функционирования таких систем вызывает серьезные трудности, связанные со сложностью информационных процессов и участием человека как неотъемлемого звена функционирования СТИС, которое характеризуется большой неполнотой и недостоверностью информации, множеством дестабилизирующих факторов, влияющих на СТИС, приводящих к поступлению в систему новой для нее информации. Причиной проявления дисфункционального поведения СТИС являются проблемы объединения решений технико-технологической и социальной системы в социотехническую и проблемы согласования организационно-управленческих задач.

Цель подхода СТИС – формировать организации на основе совместной оптимизации. Под этим подразумевается, что СТИС будут функционировать наилучшим образом только тогда, когда социальная и техническая системы построены так, чтобы служить потребностям друг друга, что обеспечит повышение устойчивости функционирования этих систем в целом.

2. Пирамида цифровых угроз. Генезис развития представления об эволюции содержания информационной безопасности от установления защищенности программно-аппаратных платформ ИТКС до обеспечения безопасности функционирования СТИС нашел отражение в официальном документе Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), опубликованном в феврале месяце с. г. под названием «пирамида современных взаимосвязанных сетевых угроз, вызванных применением цифровых технологий на семи уровнях информационного пространства».

Семь уровней, по классификации Роскомнадзора, от основания пирамиды до вершины, это сетевое оборудование; маршрутизация; обработка данных; сервисы; вредоносная информация; общественно-опасная информация; фейки, цензура (рис. 1).

Рис. 1. Пирамида цифровых угроз в трактовке Роскомнадзора

На каждом уровне, кроме верхнего, отдельно выделяются источники угроз и собственно угрозы. В основе пирамиды лежат угрозы сетям связи, интернет-маршрутизации и конфиденциальности данных. На вершине – контентные и смысловые угрозы, связанные общественным сознанием.

Иностранное происхождение цифровых угроз в пирамиде Роскомнадзора впрямую упоминается семь раз. На базовом уровне это – импорт оборудования передачи данных и голоса, обслуживание устройств из-за рубежа. На уровнях более высокого порядка – нахождение за границей и контроль со стороны США над системами маршрутизации трафика и адресации интернета. Еще выше – обработка данных на серверах, расположенных за рубежом, иностранные ключи и алгоритмы шифрования, затем – контроль американскими компаниями магазинов приложений, соцсетей, мессенджеров, видеохостингов, сервисов и библиотек разработчиков.

Если учесть, что угрозы на верхних уровнях пирамиды Роскомнадзор не называет иностранными, но подразумевает, что они тоже исходят из-за рубежа (пропаганда экстремизма и терроризма, искажение информации, ограничение свободы слова, подрыв традиционных ценностей), то мы должны согласиться с тем, что главный фокус противодействия рискам в сфере ИКТ власти и население России должны направлять вовне.

«Ключевые системы, обеспечивающие маршрутизацию трафика и адресацию в сети Интернет, находятся за рубежом, управляются организациями, контролируемыми США. Данные обрабатываются на серверах, находящихся за рубежом, пользовательские устройства находятся под управлением обновляемых дистанционно из-за рубежа ОС, применяются иностранные ключи и алгоритмы шифрования», – говорится в инфографике.

Это угрожает отказами в обслуживании и модернизации оборудования и пользовательских устройств, перехватом управления, несанкционированным сбором данных и нарушением работы критической инфраструктуры связи, отмечается на сайте ведомства.

Также в числе источников угроз названо то, что «магазины приложений, соцсети, мессенджеры, видеохостинги, сервисы и библиотеки разработчиков находятся за рубежом и контролируются американскими компаниями». Из-за этого, по мнению ведомства, возможны отказы в размещении в магазинах приложений, блокировка пользовательских аккаунтов, деанонимизация и локализация пользователей, отказ в работе библиотек и внедрение

цифровых «закладок». Роскомнадзор в инфографике предупреждает и о возможной недоступности ресурсов, связанной с зарубежным контролем над серверами, перегрузки сети и искажении маршрутов трафика, связанных с источниками опасности.

«Искажение информации, ограничение свободы слова и права получать информацию, манипуляция общественным сознанием, подрыв традиционных ценностей», по мнению Роскомнадзора, – главная из «смысловых угроз, связанных с манипуляцией интернет-платформами общественным сознанием». Ее источник – вредоносная и общественно-опасная информация: распространение детской порнографии, наркотиков, призывов к самоубийству, пропаганда экстремизма и терроризма, призывы к массовым беспорядкам и другие ее виды, отметили в ведомстве.

Надо признать, что такой подход к определению семиуровневой пирамиды цифровых угроз в силу их универсальности и трансграничности можно распространить и на все информационное пространство Союзного государства.

3. Коллективная информационная безопасность Союзного государства. В настоящее время, безусловно, каждое государство по отдельности уже создало свою национальную нормативную и законодательную базу в области обеспечения ИБ своего государства. Также, очевидно, что она постоянно совершенствуется и конкретизируется. Но мы должны четко понимать, что обеспечение национальной ИБ в рамках своего «удельного» законодательства еще не гарантирует защиту от новых вызовов и угроз в силу того, что мир, в котором мы живем, чрезвычайно изменился и, прежде всего, благодаря появлению новых сетевых информационных технологий осуществления трансграничных коммуникаций между народами и странами в едином глобальном информационном пространстве. Ему свойственны новые ранее отсутствующие характеристики:

– глобальность (каждый с каждым практически единомоментно);

– трансграничность (отсутствие границ в информационном пространстве;

– моментальность распространения информационных сообщений (благодаря глобальной информационно-телекоммуникационной инфраструктуре сети Интернет; появление новых средств коммуникаций посредством социальных ресурсов Интернет (СС, блогосфера, Twitter, мессенджеры и др.); а также повышенной доступности средств глобального общения: сотовой связи, коммуникаторов, спутникового телевидения прямого вещания;

– эффективность средств медийного манипулирования психологией как индивида, так и социума в целом;

– наличие надгосударственных структур, по-сути, управляющих современным международным сетевым информационным пространством (Twitter, YouTube, Facebook, мессенджеры и др. инструменты информационных транснациональных коммуникаций).

Природа этих глобальных изменений в общепланетарном одна – появление глобального информационного общества, где потенциально существует возможность организации информационной связи каждого с каждым. Именно такое содержание предметной области и определяет необходимость разработки нового подхода к разработке Концепции коллективной информационной безопасности Союзного государства

Это уже не просто гармонизация национальных законодательных актов в области обеспечения ИБ своих государств, но это формирование общего подхода к обеспечению именно коллективной ИБ единого информационного пространства, объединяющего наши народы. Важно, что именно объединяющего, и ни в коем случае не разъединяющего наши народы. А попытки сделать его именно разъединяющим мы все чувствуем практически повседневно.

Надо отметить, что наши оппоненты в лице стран НАТО уже давно это осознали и создали ряд Центров, предназначенных именно для коллективного взаимодействия в области обеспечения ИБ информационного пространства стран НАТО.

Однако, обращаясь к предмету регулирования, мы отмечаем, что обеспечение ИБ Союзного государства только в рамках национального законодательства уже НЕДОСТАТОЧНО (!), так как эти угрозы имеют трансграничный характер. К сожалению, последние события на территориях государств-членов ОДКБ, еще более заострили необходимость именно

такой трактовки КБ. Именно в силу того, что современное информационное пространство имеет трансграничный характер и, как показали события в Беларуси, угрозы информационной безопасности, проявленные относительно одного государства, входящего в ОДКБ, имеют не только национальное проецирование, но, как следует из озвученной программы действий незаконно созданного Координационного совета оппозиционных сил, управляемого извне, четко обозначили угрозу всему военно-политическому союзу государств – членов ОДКБ, обозначив одной из главных целей – выход Беларуси из ОДКБ. Таким образом, была четко обозначена реальная угроза всему информационному пространству ОДКБ, т. е. коллективной безопасности ОДКБ. А это уже прямая угроза не только национальному суверенитету Беларуси, но прямая угроза для всех государств, скрепивших своей подписью необходимость обеспечения коллективной безопасности общего пространства стран ОБКБ.

Т. е. мы констатируем, что обеспечение ИБ каждого государства – это не только правовые, инструментальные и организационные вопросы отдельного государства, но есть нечто большее, что имеет признаки и свойства коллективной защиты, что не является безусловным в рамках национального законодательства. Т. е. целое (ИБ ОДКБ) обладает свойствами, которыми не обладают составляющие его части (национальные законодательства в области регулирования вопросов ИБ в отдельно взятой стране).

Таким образом, понятие «коллективная информационная безопасность» с одной стороны, признает юрисдикцию национальных законодательных актов в области обеспечения информационной безопасности, а с другой – учитывает многомерный характер международной безопасности и устанавливает определенную иерархию приоритетов и нацеливает акторов ОДКБ на совместное решение первоочередных задач.

Заключение. 1. Вопросы обеспечения информационной безопасности многосвязных распределенных во времени и пространстве сетевых объектов начинают основываться на понятии «социо-киберфизические системы»

2.Подход Роскомнадзора к определению семиуровневой пирамиды цифровых угроз в силу их универсальности и трансграничности можно распространить и на все информационное пространство Союзного государства.

3. Реальные трансграничные угрозы в глобальном информационном пространстве определяют необходимость формирования Концепции коллективной информационной безопасности Союзного государства.

УДК 343.3

СОВЕРШЕНСТВОВАНИЕ ВЗАИМОДЕЙСТВИЯ ЭКСПЕРТА ВНЕСУДЕБНОЙ ОРГАНИЗАЦИИ И СЛЕДОВАТЕЛЯ ПРИ ПРОВЕДЕНИИ ЭКСПЕРТИЗЫ ЭКСТРЕМИСТСКИХ ИНФОРМАЦИОННЫХ МАТЕРИАЛОВ

А.В. ИВАНОВСКИЙ
Академия МВД Республики Беларусь, г. Минск

Введение. В течение 2020–2021 гг. лидеры и иные организаторы мятежа активно выступали с призывами, оказывая деструктивное информационное воздействие (далее − ДИВ) на граждан, общество и государство. В настоящее время в Беларуси реализуется комплекс мер по информационному противодействию «цветной революции» [1,2], в том числе выполняются и действия, предусматривающие ***неотвратимость наказания всех лиц,*** которые совершили поступки, выходящие за пределы национального правового поля.

В белорусском законодательстве под ДИВ понимают «осуществление информационного влияния на политические и социально-экономические процессы, деятельность государственных органов, а также на физических и юридических лиц в целях ослабления обороноспособности государства, нарушения общественной безопасности, принятия и заключения заведомо невыгодных решений и международных договоров, ухудшения отношений с другими государствами, создания социально-политической напряженности, формирования угрозы возникновения чрезвычайных ситуаций, разрушения традиционных духовных и нравственных ценностей, создания препятствий для нормальной деятельности государственных органов, причинения иного *ущерба национальной безопасности*» [3, абз.5, п.8]. Проблема влияния ДИВ на национальную безопасность (далее − НБ) должна рассматриваться через призму коммуникаций, проведения пропаганды и агитации с использованием современных методов и технологий. Поведение и действия участников протестов ими же тщательно фиксировались, а затем распространялись в сети интернет, печатных изданиях. Эти сведения позволили сформировать доказательную базу для работы следственных органов.

Уже к началу 2020 г. на белорусском направлении была создана информационная группировка прозападных сил, включавшая 32 аналитических центра, 45 СМИ, 91 НКО, 244 блогера и эксперта, разветвленные социальные сети. Это позволило им резко повысить интенсивность и токсичность выпускаемых информационных материалов. Так, только у десяти ведущих блогеров в период 2014–2019 гг. эти показатели выросли в 8 раз. В институтах государства, в экономике, социальной и культурной сферах, различных группах общества формировались структуры и вербовались сторонники т.н. называемых «перемен».

Для сторонников протестов были сформированы «информационные коконы». С начала августа 2020 г. представители оппозиции приступили к активной и открытой антиправительственной агитации. Одновременно число задействованных для этой цели информационных ресурсов возросло почти вдвое, к работе подключились также граждане и военнослужащие зарубежных стран. При коммуникациях максимально использовались агрессивные приемы выступления в аудиториях, коммуникационной полемики на форумах: «смотреть свысока; использовать драматизирующие ситуацию полемические обороты; приписывать властям только дурные качества; констатировать отсутствие интеллекта силовикам и госслужащим; отрицать наличие всего; подменять реальные факты надуманными; глумится над подходом к проблемам своих оппонентов оппонента; хитрость, т. е. говорить не по существу обсуждаемого вопроса, свидетельствовать, используя ссылки на западные авторитетов, заявлять «доколе ...», «это уже давно известно»; не допускать, чтобы оппонент был хоть в чем-нибудь прав; покидать поле дискуссии с видом безусловного победителя» [4, с. 111].

Общая численность протестующих и сочувствующих им лиц в августе превышала 10 % от общей численности избирателей (более 6,7 млн чел). К инновациям в «цветных» политических технологиях во время мятежа в Беларуси следует отнести следующие:

1. Мятеж в Беларуси – составная часть проведения комплексной цветной революции на постсоветском пространстве, информационное воздействие организаторов мятежа о ходе протестов велось на глобальную аудиторию.

2. Протест был рассредоточен в геополитическом пространстве. Законспирированный центр управления размещался за границей, целеуказание протестующим и коммуникации с ними велись с зарубежных информационных платформ, указания подогревались оппозиционными белорусскими сайтами. В местах проведения протестных акций действиям руководили лишь организаторы нижнего звена.

3. Мятеж был направлен не только на смещение действующего Главы государства, но и смену существующего государственного строя.

4. В протесты вовлекались коллективы валообразующих государственных промышленных предприятий. Правда, численность забастовок была не велика – 237 человек (из 45 000 работников предприятий), профсоюз стачкомовцев составил всего 5 человек.

5. В Интернет и ТГ-каналах в качестве инструмента быстрого и массового вовлечения людей в протест комплексно использовались недостоверная информация, манипулирование, «вирусное распространение», «снежный ком», «цепная реакция» и проч.

6. Компенсация незначительных размеров «толпы на площади» в СМИ дополнялась формированием в информационном потоке эффекта массовости сообщений за счет большого числа иных «массовых» точек протеста.

7. У участников протестов последовательно менялась мотивация:

7.1. «Ужасен не сам факт фальсификации, а ее масштаб» (фотографии множества протоколов нарушений);

7.2. «Подавление мирного протеста осуществлялось с особой жесткостью» (социальные сети захлестнул поток свидетельств насилия, репортажей выхода из СИЗО участников протеста);

7.3. «В протестах участвуют все» (создание информационного фона массовости протестов).

8. Тактика действий на различных этапах протеста была достаточно гибкой.

8.1. На этапе подъема протестной активности: вывод на улицы массы без лидеров и партий; использование лидеров мнений в качестве катализаторов протестов (спортсмены, артисты, и др.); переформатирование влияния протестных групп по ходу мятежа, передача управления протестом радикалам сразу после проведения голосования;

8.2. На этапе спада: вовлечение в протесты женщин, пенсионеров, инвалидов, подростков и детей; оживление деятельности организаций националистов для долгосрочной политической деятельности в будущем;

8.3. На завершающем этапе предпринимались попытки проведения диверсий на железной дороге, шоссейных дорогах, поджоги государственных организаций и т. д.

Анализ прошедших событий и их последствий позволяет говорить о нанесении существенного ущерба НБ. Перечень призывов к действиям, направленным на причинение вреда НБ, представлен в **ст. 361** Уголовного кодекса Республики Беларусь (далее − УК). Часть деяний непосредственно перечислена в этой статье УК: публичные призывы к захвату государственной власти, или насильственному изменению конституционного строя Республики Беларусь, или измене государству, или совершению акта терроризма или диверсии (абз. 1 ст. 261 УК); призывы, обращенные к иностранному государству, иностранной или международной организации, совершить действия, направленные на причинение вреда национальной безопасности Республики Беларусь, либо распространение материалов, содержащих такие призывы (абз. 2 ст. 261 УК); действия, совершенные с использованием средств массовой информации или глобальной компьютерной сети Интернет (абз. 3, ст. 261 УК).

Пример. В видеозаписи официального заявления лидера протестов М.Колесниковой, размещенной на интернет-ресурсе 14.08.2020, говорилось о том, что «*Светлана Тихановская одержала победу на выборах 9 августа. Бывший Президент должен подать в отставку*».

В этом заявлении несложно усмотреть последствия прямого призыва к признанию результатов президентских выборов недействительными. При этом случае действующий Глава государства становится нелегитимным; он не признается Президентом страны, должен уйти в отставку или быть отстранен от власти. После этого необходимо провести не предусмот-

ренный избирательным законодательством пересчет голосов избирателей и пересмотр результатов выборов. После должен начаться процесс передачи власти Тихановской С.Г. от действующего Главы государства.

В случае реализации этого призыва создавались реальные условия для неконституционного захвата власти в Республике Беларусь. При этом М. Колесникова использовала недостоверную информацию и вводила в заблуждение часть граждан. Очевидно, что этот призыв попадает под действие аб. 1 ст. 361 УК «захват государственной власти» со всеми вытекающими правовыми последствиями.

Отдельно стоит вопрос о перечне «***иных действий***, направленных на причинение вреда НБ Республики Беларусь», указанных абз. 1 ст. 261 УК. Для решения этой задачи разработана экспертная методика, позволяющая вести анализ информационных материалов на предмет наличия в них заявлений, представляющих угрозу НБ, ориентированная на ст. 361 УК. Для этого выполнялись следующие действия:

1. Составлен перечень терминов и понятий, необходимых для отнесения экспертами призывов и действий к сфере национальной безопасности с использованием нормативных и правовых актов, научной и учебной литературы.

2. Сформирован список источников и угроз, для чего последовательно выделялись [5]:

2.1 перечни национальных интересов в сферах НБ (политической, экономической, социальной, информационно, демографической, военной);

2.2. перечни источников угроз в каждой сфере НБ;

2.3. перечни потенциальных и реальных угроз в сферах НБ.

3. Проведен экспертный анализ призывов к действиям участников протестов и их соотнесение со списком источников и угроз в сферах национальной безопасности. Вначале устанавливались факты того, что действия и призывы, содержащиеся в представленных материалах, являлись источниками и трансформировались в угрозы НБ. При этом акцент был сделан на *установление фактов не того, о чем автор думал в момент выступления, а того, что именно он сказал, т. е.* ***установления конечной цели*** *высказываний.*

В случае необходимости следователю вносились предложения по встраиванию выводов экспертов в формулу обвинения с учетом дополнительных к 361 ст. статей УК.

Приведем примеры формулировок фрагментов формулы обвинения. Призывы и выдвигаемые основания для захвата власти создали *реальные угрозы национальной безопасности***,** перечень которых включал:

– посягательство на независимость, территориальную целостность, суверенитет и конституционный строй Республики Беларусь [5; п.,27, абз. 2];

– навязывание Республике Беларусь политического курса, не отвечающего ее национальным интересам, вмешательство извне во внутриполитические процессы [5; п. 27, абз. 3];

– проявление социально-политического экстремизма и вражды на территории Республики Беларусь [5; п. 27, абз. 14];

– возникновение в Республике Беларусь беспорядков, сопровождающихся насилием либо угрозой насилия со стороны группы лиц и организаций, в результате которых возникает опасность жизни и здоровью людей, независимости, территориальной целостности, суверенитету и существованию государства [5; п. 27, абз. 15];

– дезорганизацию системы государственного управления, создание препятствий функционированию государственных институтов [5; п. 27, абз. 16];

– деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам [5; п. 27, абз. 20];

– утрату значительной частью граждан традиционных нравственных ценностей и ориентиров, попытку разрушения национальных духовно-нравственных традиций и необъективного пересмотра истории, затрагивающие данные ценности и традиций [5; п.27, абз. 26];

– резкое и масштабное снижение доверия граждан к основным государственным институтам [5; п. 27, абз. 27].

При публичном выступлении и размещении его содержания в сети Интернет, иных каналах коммуникаций лидеры протестного движения своими призывами оказывали на аудиторию ДИВ: вели антиправительственную агитацию, проводили указание целей и направления желаемых действий. Публичные выступления тиражировались средствами массовой информации или глобальной компьютерной сетью Интернет. На митингах и пресс-конференциях направленность агитации и призывов осознавалась их участниками, о чем свидетельствуют поддерживающие выступление коллективные выкрики, высказывания и задаваемые журналистами вопросы, в сетевом сообществе отметка выступлений лайками, перепостами, обсуждениями на форумах.

Исследование информационных материалов, размещенных с сети Интернет, показало, что совокупность выступлений и направленность призывов лидеров протестов ДИВ в Беларуси использовала практически все составляющие модели социально-психологического воздействия на личность и общество [6]; опиралась на методологию и технологии «цветных революций» [7].

Эти действия для формирования синергии использовали:

– согласованный по целям, задачам, времени, пространству состояниям, задействованным ресурсам характер;

– использовали специализацию исполнителей и их взаимное дополнение;

– сыграли важную роль в драматизации происходящих событий и изменению сознания коммуникационных аудиторий;

– выводила смыслы и содержание призывов за пределы действующего правового поля Республики Беларусь; опиралась на технологии искусственного интеллекта [8].

В конечном итоге действия агитаторов, распространяемые электронными и печатными СМИ, глобальной компьютерной сетью Интернет, они обеспечили деструктивную подчиняемость и девиантное поведение части населения Беларуси в период протестных акций.

Заключение. Требуется вывести белорусское общество из психологического шока, вызванного попыткой неконституционного захвата власти, обеспечить стабильность развития государства в сложнейшей и динамично меняющейся геополитической обстановке.

Необходимо разрушить организационную и технологическую инфраструктуру ведения «цветной революции», привлечь к ответственности не только лидеров протестов, но и всех организаторов среднего и нижнего звена, исполнителей противоправных действий.

Общество должно быть уверено в том, что поступки и деструктивные действия, наносящие ущерб НБ и выходящие за пределы национального правового поля, неотвратимо будут наказаны.

Список литературы

1. Overextending and Unbalancing Russia. ASSESSING THE IMPACT OF COST-IMPOSING OPTIONS [Электронный ресурс].Режим доступа : http:// RAND_RB1001420(1).pdfP.4. – Дата доступа : 13.04.2021.

2. ИА REGNUM [Электронный ресурс]. – Режим доступа : http://www.regnum.ru/news/polit/1887990.html#ixzz3REbXovzG. – Дата доступа : 25.01.2015.

3. О Концепции информационной безопасности Республики Беларусь : Пост. Совета безопасности Респ. Беларусь, 18 марта 2019 г., № 1 [Электронный ресурс] // Национальный правовой Интернет-портал Респ. Беларусь, 20.03.2019, 7/4227. Режим доступа : https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf. – Дата доступа : 13.04.2021.

4. Бунт. Учебник активиста. – М., 2007. − 204 с.

5. Об утверждении Концепции национальной безопасности Республики Беларусь : Указ Президента Респ. Беларусь, 9 нояб. 2010 г., №575 [Электронный ресурс] // Нац. центр правовой информ. Респ. Беларусь. – Режим доступа : www.pravo.by. – Дата доступа : 25.03.2021.

6. Занковский, А. Н. Модель психологического воздействия в социальных сетях / А.Н. Занковский, В. В. Латынов // Организационная психология и психология труда / Институт психологии Рос. акад. наук. – Режим доступа : http://work-org-psychology.ru/engine/documents/document637.pdf. – Дата доступа : 13.04.2021.

7. Государственная политика информационной безопасности и информационное противоборство : учеб. пособие / В. Ю. Арчаков [и др.]. – Акад. управл. при Президенте Респ. Беларусь. – Минск : – 2020, 245 с.

8. Нестик, Т. А. Информационные войны с использованием систем искусственного интеллекта: анализ психологических механизмов воздействия / Т. А. Нестик, Е. А. Михеев // Институт психологии Российской академии наук. Организационная психология и психология труда. – 2019. – Т. 4, № 4. – С. 148–174.

СЕКЦИОННЫЕ ЗАСЕДАНИЯ

ЗАСЕДАНИЕ № 1
ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 621.396; 534.41

ДОСТОВЕРНОСТЬ ОЦЕНКИ ПАРАМЕТРОВ СЛОЖНЫХ СИГНАЛОВ ПРИ ДИСКРЕТНОМ ПРЕОБРАЗОВАНИИ

В.К. ЖЕЛЕЗНЯК, И.Б. БУРАЧЕНОК, С.В. ЛАВРОВ
Учреждение образования «Полоцкий государственный университет», г. Новополоцк, Республика Беларусь
А.Г. ФИЛИППОВИЧ, М.М. БАРАНОВСКИЙ
Оперативно-аналитический центр при Президенте Республики Беларусь, г. Минск

Введение. До недавнего времени из-за существования довольно простых способов генерирования различных сложных сигналов, например, использование обычных аналоговых схем, в практике спектрального анализа основное место занимали гармонические базовые функции. Однако широкое распространение программных средств цифровой обработки сигналов открыло возможность проведения анализа различного рода кривых практически в любой базисной системе. Цифровые, или, как их часто называют дискретные методы анализа, вызывают наибольший интерес у специалистов, так как чем меньше интервал дискретизации (чем выше частота дискретизации), тем точнее отображается исходная функция (форма восстановленного сигнала приближается к оригиналу), и тем меньше ошибки квантования сигналов [1]. Несмотря на то, что при этом увеличивается и количество обрабатываемой информации, что требует увеличения как объема памяти, так и быстродействия устройства обработки информации возможности современных вычислительных систем делают это направление актуальным.

Целью представленного в статье исследования является повышение достоверности оценки параметров сложных сигналов при дискретном преобразовании.

Основными подлежащими решению являются задачи исследования математических методов оценки параметров сложных систем и возможностей повышения точности оценки параметров сигналов, которые позволяют при надлежащем выборе формы сигнала найти основные динамические характеристики исследуемой системы.

Базисной системой называют систему функций $\{f_k(t)\}$, а представление кривой в виде суммы функций $X(t) = \sum_{k=0}^{\infty} a_k f_k(t)$ называется ее разложением по системе базисной функций. Для выбранной системы функций кривая может быть полностью охарактеризована набором весовых коэффициентов $\{a_k\}$ или зависимостью $a(k)$, а одна и та же кривая в зависимости от выбранной системы базисных функций может иметь кривые различных типов. Любую сложную функцию в соответствии с методами линейной теории можно аппроксимировать суммой более простых функций, обладающих ортогональностью. Разложение функций возможно по различным системам: разложение по системе непрерывных ортогональных функций; разложение по системе дискретных функций (конечное число отсчетов); разложение тригонометрических функций, разложение по системе дельта-функций и др. [2].

Далее остановимся на исследовании разложения по системе дельта-функций. Дискретным называется сигнал, квантованный по уровню и по времени (или по уровню и времени одновременно). При квантовании по уровню все возможные значения сигнала в каждый момент времени представляются некоторым конечным числом разрешенных уровней, отстоящих друг от друга на конечные интервалы. Дискретизация сигналов может приводить к определенной потере информа-

ции о поведении сигналов в промежутках между отсчетами. Однако существуют условия, определенные теоремой Котельникова, согласно которой аналоговый сигнал с ограниченным частотным спектром может быть без потерь информации преобразован в дискретный сигнал, и затем абсолютно точно восстановлен по значениям своих дискретных отсчетов [2]. Однократно квантованный сигнал (т. е. квантованный только по уровню или только по времени) иногда рассматривают как дискретно-непрерывный, считая дискретным только сигнал, одновременно квантованный как по уровню, так и по времени [3]. В системах цифровой обработки данных сигнал всегда является цифровым, так как представлен с точностью до определенного количества разрядов. Поэтому при описании цифровых сигналов функция квантования обычно опускается (подразумевается равномерной по умолчанию), а для описания сигналов используются правила описания дискретных сигналов. Множество значений непрерывной кривой, полученное в процессе ее дискретизации по временной оси, обусловливает получение дискретного сигнала. Способ дискретизации непрерывной кривой определяется фиксированным количеством временных отсчетов одинаковой длительностью по оси времени. Примером дискретного сигнала с квантованием по времени является модулированная по амплитуде последовательность идеальных импульсов.

Идеальный единичный импульс рассматривается как сигнал в виде так называемой дельта-функции [3], свойства которой определяются отношениями:

$$\delta(t-\xi)=\begin{cases}0 & \text{при } t\neq\xi\\ \infty & \text{при } t=\xi\end{cases} \tag{1}$$

$$\int_a^b f(t)\delta(t-\xi)dt = f(\xi), \tag{2}$$

где $\delta(t-\xi)$ – дельта-функция, t – время, ξ – момент действия импульса, a и b – произвольные действительные числа (в том числе и $\pm\infty$).

Представленная математическая модель идеализирует реальный импульс в том смысле, что определяет его длительность равной нулю, а уровень – равный бесконечности, что сразу исключает из рассмотрения эти параметры. Однако «площадь» такого идеализированного импульса конечна и равна единице, так из (2) при $f(t)=1$ следует

$$\int_a^b \delta(t-\xi)dt = f(\xi),\ \ a<\xi<b, \tag{3}$$

Таким образом, единственным параметром этого сигнала является момент его действия ξ. Если положить, что $a=0$, $b=t$, то из (3) получим

$$\int_0^t \delta(t-\xi)dt = 1,\ \ a<\xi<b, \tag{4}$$

откуда следует, что интегрирование сигнала в виде дельта-функции дает постоянную величину, равную единице.

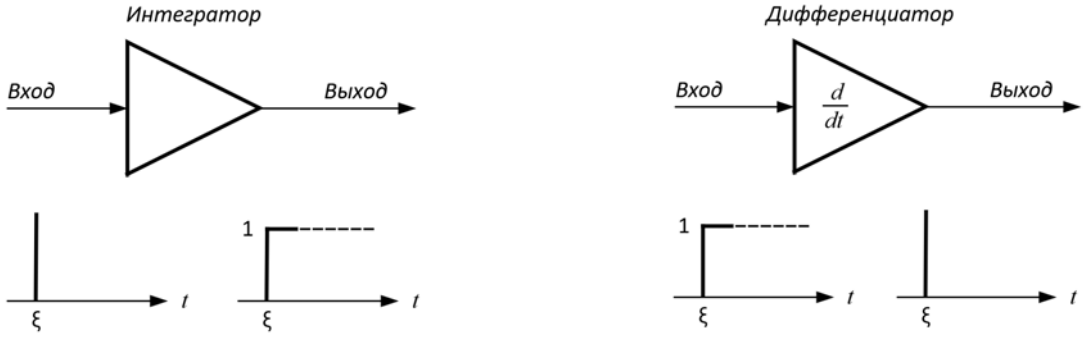
Так как импульс действует в момент времени $t=\xi$, значение интеграла отлично от нуля для $t>\xi$ (символически можно обозначить единичной функцией $1(t-\xi)$ [3]). Тогда выражение (4) можно записать следующим образом

$$\int_0^t \delta(t-\xi)dt = 1(t-\xi). \tag{5}$$

Если продифференцировать выражение (5) по времени, получим

$$\delta(t-\xi) = \frac{t}{dt}1(t-\xi). \tag{6}$$

Таким образом, если подать на вход интегратора сигнал, представленный дельта функцией, то на выходе получим сигнал в виде единичной функции (рис. 1, *а*). Подача на вход дифференциатора единичной функции на выходе дает дельта-функцию (рис. 1, *б*).

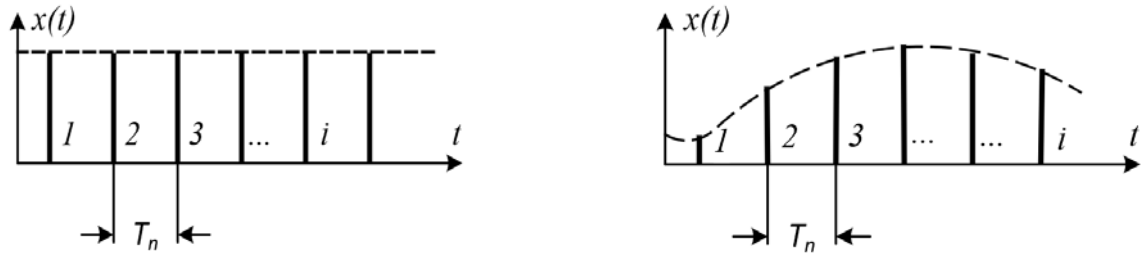


а – формирование единичной функции *б* – формирование дельта функций

Рис. 1. Модели формирования единичной и дельта-функций

Это доказывает то, что масштаб единичной функции можно изменить любым образом, достаточно лишь умножить ее на любую постоянную величину. При этом дельта-функция будет иметь тот же постоянный множитель, обозначающий изменение «площади» дельта-функции в соответствующее число раз (по сравнению с единицей) [3].

С помощью дельта-функций можно представить идеализированную последовательность импульсов постоянного или переменного уровней с интервалами следования T_n, как показано на рис. 2.



а *б*

Рис. 2. Идеализированная последовательность импульсов с постоянными интервалами следования: *а* – постоянного уровня; *б* – переменного уровня

В первом случае можно записать:

$$x(t) = \sum_{i=1}^{N} a\delta(t - i\mathrm{T}_n). \tag{7}$$

Во втором случае:

$$x(t) = \sum_{i=1}^{N} x(i\mathrm{T}_n)\delta(t - i\mathrm{T}_n). \tag{8}$$

При этом следует иметь в виду символический характер множителей а в формуле (7) и $x(i\mathrm{T}_n)$ в формуле (8), которые определяют «площади» соответствующих дельта-функций (так как уровни дельта-функций бесконечно велики).

В настоящее время в большинстве случаев произвольный детерминированный сигнал представляется в виде совокупности элементарных сигналов. Известно, что всякая функция $x(t)$, удовлетворяющая на промежутке $0 \le t \le T$ условиям Дирихле:

а) интервал, на котором функция определена, может быть разбит на конечное число интервалов, в каждом из которых функция $x(t)$ непрерывна и монотонна;

б) во всякой точке разрыва функции $x(t)$ существуют значения $x(t+0)$ и $x(t-0)$); может быть разложена в ряд Фурье, т. е. представлена точно или приближенно суммой гармоник с соответствующими постоянными коэффициентами.

Таким образом, если функция $x(t)$ имеет конечную длительность, то она может быть представлена суммой элементарных детерминированных сигналов типа синусоиды. При этом каждый элементарный сигнал характеризуется своей амплитудой (можно определить по формуле $C_k = \frac{1}{T}\int_0^T x(t)e^{-2\pi kj\frac{t}{T}}dt$), и частотой $\frac{2\pi k}{T} = \omega_k$. Расстояние между соседними частотами гармоник по оси частот равно $2\pi/T$.

Разложение функции $x(t)$ на бесконечную последовательность дельта-функций с «площадями», определяемыми соответствующими значениями самой же разлагаемой функции имеет большое значение в теории линейных систем, так как позволяет определять реакцию системы на произвольный входной сигнал простой суперпозицией более простых реакций на воздействие в виде дельта-функций.

Математически дискретные сигналы представляются в виде непрерывных последовательностей чисел – дискретных функций. Например, квантование по времени заменяет непрерывную функцию решетчатой, которая определяется совокупностью выделенных ординат, или дискрет. Эти ординаты, или дискреты, модулируют некоторую последовательность импульсов. Решетчатой называют функцию $f[nT]$, заданную дискретными значениями через равностоящие интервалы времени, т. е. В моменты времени $0, T, 2T, ...$ [4], например, как показано на рис. 3.

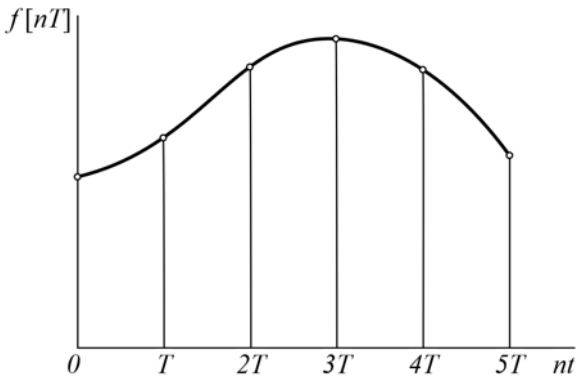


Рис. 3. Решетчатая функция

В промежутки времени функция $f[nT]$, равна нулю. Число может n принимать целые положительные значения. Решетчатую функцию (РФ) можно образовать из любой числовой таблицы. Ее можно образовывать и из непрерывной функции, придавая ее аргументу кратные T значения. При переходе от непрерывной функции к решетчатой масштаб времени изменяют таким образом, чтобы интервал времени между смежными значениями аргумента равнялся 1. Например, если задана непрерывная функция $f(t) = \mathrm{e}^{a_1 t}$, то введя время $\bar{t} = \frac{t}{T}$, получим $f(\bar{t}) = \mathrm{e}^{a\bar{t}}$, где $a = a_1 T$. РФ обозначается либо как $f[nT]$, либо как $f[n]$. Одной и той же решетчатой функции $f[n]$ может соответствовать несколько непрерывных функций.

Поиск и установление сложных систем с помощью математической модели исследуемого объекта реализуется на основе определения входных воздействий и откликов. Точность модели обеспечивается высокой точностью измерений ее определяющих параметров.

Далее подробно остановимся на разности k-го порядка РФ. В теории РФ огромную роль играет разность 1-го порядка [5]

$$\Delta f[n] = f[n+1] - f[n] \tag{9}$$

$\Delta f[n]$ равно приращению РФ при переходе от аргумента n к аргументу $n+1$.

Разность 2-го порядка

$$\Delta^2 f[n] = \Delta f[n+1] - \Delta f[n] = f[n+2] - f[n+1] - f[n+1] + f[n] = f[n+2] - 2f[n+1] + f[n]. \tag{10}$$

Разность k-го порядка [5]

$$\Delta^k f[n] = \sum_{\nu=0}^{k} (-1)^{\nu} \frac{k!}{\nu!(k-\nu)!} f[n+k-\nu]. \tag{11}$$

В качестве примера рассмотрим

1. функцию $f[n]=an^2$ – в соответствии с (9) для нее

–первая разность записывается $\frac{f[n]}{a}=(n+1)^2-n^2=2n+1;$

–вторая разность записывается $\frac{\Delta^2 f[n]}{a}=(n+2)^2-2(n+1)^2+n^2=2.$

2. функцию $f[n]=e^{an}$ – в соответствии с (9) для нее

–первая разность записывается $f[n]=e^{a(n+1)}-e^{an}=e^{an}(e^a-1);$

–вторая разность записывается $\Delta^2 f[n]=e^{a(n+2)}-2e^{a(n+1)}+e^{an}=e^{an}(e^a-1)^2.$

Из теории уравнений в конечных разностях, рассмотренной в книге Я.З. Цыпкина [5] уравнением p-го порядка в конечных разностях, или разностным уравнением p-го порядка называют уравнение, в которое входят неизвестная функция $y=[n]$ и ее разности до p-го порядка включительно:

$$b_p\Delta^p y[n]+b_{p-1}\Delta^{p-1}y[n]+...+b_0 y[n]=f[n], \tag{12}$$

где $b_p, b_{p-1},...$ – коэффициенты; $f[n]$ – внешняя сила, воздействующая на систему.

Существует и вторая форма уравнений в конечных разностях. Ее получают из (12) , заменяя все разности (начиная с $\Delta y[n]$ и заканчивая $\Delta^p y[n]$) на их выражениях через $y[n+1],\ y[n+2],\ \ldots,\ y[n+p]$, в соответствии с формулой (11).

Если затем объединить слагаемые с одинаковыми значениями аргументов функции y, т. е. слагаемые с $y[n],\ y[n+1],$ вплоть до $y[n+p],$ то получим следующее

$$a_p y[n+p]+a_{p-1}y[n+p-1]+...+a_0 y[n]=f[n], \tag{13}$$

Уравнение в конечных разностях в отличие от дифференциальных уравнений обладает особенностями:

1) записанное в виде (13) оно позволяет определять последующие значения отклика системы $y[n+p]$ через значения отклика в предыдущие моменты времени, т. е. через значения $y[n+p-1], y[n+p-2],...,$ вплоть до $y[0]$ и через значения вынуждающей силы $f[n]$.

2) если условно называть порядком разностного уравнения разность максимального и минимального значения аргументов функции y этого уравнения, то порядок разностного уравнения не всегда совпадает с порядком наивысшей разности того же уравнения.

Заключение. В работе показано, что любую сложную функцию в соответствии с методами линейной теории можно аппроксимировать суммой более простых функций, обладающих ортогональностью, каждая из которых несет только свою долю информации, содержащейся в кривой. Установлено, что одни и те же функции можно разложить не только по синусам и косинусам, но и по другим ортогональным базисным системам. В частности, в качестве ортогональных функций могут быть использованы различного типа многочлены. Дискретный сигнал в процессе его анализа может быть разложен только по системам дискретных базисных функций, у которых отсчеты времени совпадают с отсчетами сигнала. Наиболее значимые результаты получены с использованием разложения непрерывной функции на дельта-функции.

Список литературы

1. Бураченок, И. Б. Обнаружение первичных признаков речевого сигнала / И. Б. Бураченок, В. К. Железняк // Вестник Полоцкого государственного университета. – 2020. – № 12. – С. 2-12.

2. Анцыферов, С. С. Общая теория измерений : учеб. пособие / С. С. Анцыферов, Б. И. Голубь / под ред. Акад. РАН Н.Н. Евтихиева. – М. : Горячая линия – Телеком, 2007. – 176 с.

3. Солодов, А .В. Теория информации и ее применение к задачам автоматического управления и контроля / А. В. Солодов. – М. : Наука, 1967. – 432 с.

4. Бессонов, Л.А. Линейные электрические цепи : учеб. пособие для электротехн. и радиотехн. специальностей вузов / Л.А. Бессонов. – Изд. 2-е, перераб. и доп. – М. : Высшая школа, 1974. – 320 с.

5. Цыпкин, Я. З. Основы теории автоматических систем : учеб. пособие / Я.З. Цыпкин. – М. : Наука, 1977. – 560 с.

УДК 621.396

МЕТОДИКА ВЕРОЯТНОСТНОЙ ОЦЕНКИ РАЗБОРЧИВОСТИ РЕЧИ

А.А. ХОРЕВ, И.С. ПОРСЕВ
Национальный исследовательский университет «Московский институт электронной техники», Российская Федерация

Защита акустической речевой информации от ее утечки по техническим каналам является одной из важнейших задач обеспечения конфиденциальности переговоров, ведущихся в выделенных помещениях.

В качестве показателя оценки эффективности защиты акустической речевой информации от ее утечки по техническим каналам используется словесная разборчивость речи, под которой понимается относительное количество правильно понятых слов из перехваченного средством акустической разведки разговора.

Наиболее часто для оценки словесной разборчивости речи используется методика, предложенная Железняком Я.И., Макаровым Ю.К. и Хоревым А.А [1].

В данной методике при расчете разборчивости речи учитывается только тот случай, когда оператор услышит звуки речи во всех семи октавных полосах. Учитывая, что при низких отношениях сигнал/шум слышимость звуков речи в октавных полосах носит вероятностный характер, при прослушивании речи могут возникнуть различные комбинации октавных полос, в которых оператор может услышать звуки речи.

В работе предложена методика вероятностной оценки разборчивости речи, в основу которой положена формула полной вероятности, учитывающая вклад в разборчивость речи всех возможных комбинаций октавных полос и слышимость звуков речи в октавных полосах.

На основе экспериментальных исследований, проведенных методом артикуляционных испытаний, оценен вклад в разборчивость речи как отдельных октавных полос, так и возможных их комбинаций, а также получены зависимости слышимости тональных сигналов на среднегеометрических частотах октавных полос от отношения сигнал/шум.

В соответствие с данной методикой расчет словесной разборчивости речи проводится в следующей последовательности:

1) Измеряются уровни информативного сигнала и шума и рассчитываются отношения сигнал/шум q_i в каждой из пяти октавных полос Δf_i (со 2-й по 6-ю).

2) Рассчитывается вероятность слышимости звуков речи $P(\Delta f_i)$ в каждой из пяти октавных полос:

$$P(\Delta f_i) \approx \Phi(Q_1 \cdot q_i - Q_2),$$

где $\Phi(x) = \frac{1}{2\pi}\int_{-\infty}^{x} e^{\frac{t^2}{2}} \cdot dt$ – интеграл вероятности;

q_i – отношение сигнал/шум в i-й октавной полосе, дБ;

Q_1 и Q_2 – коэффициенты, зависящие от вида сигнала, вида шума и индивидуальных особенностей аудиторов (табл. 1).

3) Рассчитываются вероятности каждой из 32-х комбинаций октавных полос A_j, в которых оператор может услышать звуки речи $P(A_j)$ (табл. 2).

3) Для каждой комбинации A_j рассчитывается словесная разборчивость речи W_j при условии, что оператор услышит звуки речи в A_j комбинации, по формуле:

$$W_j = \mathrm{P}(A_j) \cdot \mathrm{P}(W|A_j),$$

где $P(W|A_j)$ – вероятность того, что оператор правильно распознает все слова текста при условии, что он услышит звуки речи в A_j комбинации (значения $P(W|A_j)$ приведены в табл. 3).

4) Рассчитывается словесная разборчивость речи W по формуле:

$$W = \sum_{j=1}^{N} W_j,$$

где N – количество сочетаний (комбинаций) октавных полос ($N = 2^M = 32$);
M – количество октавных полос ($M = 5$).

Таблица 1

Значения коэффициентов Q_1 и Q_2 в октавных полосах

Номер октавной полосы	Коэффициент Q_1	Коэффициент Q_2
2	0,42	– 1,24
3	0,12	– 1,43
4	0,14	– 1,20
5	0,23	– 3,32
6	0,31	– 0,54

Таблица 2

Формулы для расчета вероятности комбинаций октавных полос, в которых оператор может услышать звуки речи

Обозначение сочетания A_j	Включаемые октавные полосы f_i	Формулы для расчета вероятностей $P(A_j)$
A_0	$\varnothing$	$[1-P(\Delta f_2)] \times [1- P(\Delta f_3)] \times [1- P(\Delta f_4)] \times \times [1- P(\Delta f_5)] \times [1-P(\Delta f_6)]$
A_1	Δf_2	$P(\Delta f_2) \times [1- P(\Delta f_3)] \times [1- P(\Delta f_4)] \times \times [1- P(\Delta f_5)] \times [1-P(\Delta f_6)]$
A_2	Δf_3	$[1-P(\Delta f_2)] \times P(\Delta f_3) \times [1- P(\Delta f_4)] \times \times [1- P(\Delta f_5)] \times [1-P(\Delta f_6)]$
A_3	Δf_4	$[1-P(\Delta f_2)] \times [1- P(\Delta f_3)] \times P(\Delta f_4) \times \times [1- P(\Delta f_5)] \times [1-P(\Delta f_6)]$
A_4	Δf_5	$[1 - P(\Delta f_2)] \times [1 - P(\Delta f_3)][1 - P(\Delta f_4)] \times \times P(\Delta f_5) \times [1 - P(\Delta f_6)]$
A_5	Δf_6	$[1 - P(\Delta f_2)] \times [1 - P(\Delta f_3)] \times [1 - P(\Delta f_4)] \times \times [1- P(\Delta f_5)] \times P(\Delta f_6)$
A_6	$\Delta f_2 U \Delta f_3$	$P(\Delta f_2) \times P(\Delta f_3) \times [1 - P(\Delta f_4)] \times [1 - P(\Delta f_5)] \times \times [1- P(\Delta f_6)]$
A_7	$\Delta f_2 U \Delta f_4$	$P(\Delta f_2) \times [1 - P(\Delta f_3)] \times P(\Delta f_4) \times [1 - P(\Delta f_5)] \times \times [1- P(\Delta f_6)]$
A_8	$\Delta f_2 U \Delta f_5$	$P(\Delta f_2) \times [1 - P(\Delta f_3)] \times [1 - P(\Delta f_4)] \times P(\Delta f_5) \times \times [1- P(\Delta f_6)]$
A_9	$\Delta f_2 U \Delta f_6$	$P(\Delta f_2) \times [1 - P(\Delta f_3)] \times [1 - P(\Delta f_4)] \times \times [1- P(\Delta f_5)] \times P(\Delta f_6)$
A_{10}	$\Delta f_3 U \Delta f_4$	$[1 - P(\Delta f_2)] \times P(\Delta f_3) \times P(\Delta f_4) \times [1 - P(\Delta f_5)] \times \times [1- P(\Delta f_6)]$
A_{11}	$\Delta f_3 U \Delta f_5$	$[1 - P(\Delta f_2)] \times P(\Delta f_3) \times [1- P(\Delta f_4)] \times P(\Delta f_5) \times \times [1- P(\Delta f_6)]$
A_{12}	$\Delta f_3 U \Delta f_6$	$[1 - P(\Delta f_2)] \times P(\Delta f_3) \times [1- P(\Delta f_4)] \times \times [1- P(\Delta f_5)] \times P(\Delta f_6)$
A_{13}	$\Delta f_4 U \Delta f_5$	$[1 - P(\Delta f_2)] \times [1- P(\Delta f_3)] \times P(\Delta f_4) \times \times P(\Delta f_5) \cdot [1- P(\Delta f_6)]$
A_{14}	$\Delta f_4 U \Delta f_6$	$[1 - P(\Delta f_2)] \times [1- P(\Delta f_3)] \times P(\Delta f_4) \times \times [1- P(\Delta f_5)] \times P(\Delta f_6)$

Обозначение сочетания A_j	Включаемые октавные полосы f_i	Формулы для расчета вероятностей $P(A_j)$
A_{15}	$\Delta f_5 U \Delta f_6$	$[1 - P(\Delta f_2)] \times [1 - P(\Delta f_3)] \times [1 - P(\Delta f_4)] \times$ $\times P(\Delta f_5) \times P(\Delta f_6)$

Окончание табл. 2

Обозначение сочетания A_j	Включаемые октавные полосы f_i	Формулы для расчета вероятностей $P(A_j)$
A_{16}	$\Delta f_2 U \Delta f_3 U \Delta f_4$	$P(\Delta f_2) \times P(\Delta f_3) \times P(\Delta f_4) \times [1 - P(\Delta f_5)] \times [1 - P(\Delta f_6)]$
A_{17}	$\Delta f_2 U \Delta f_3 U \Delta f_5$	$P(\Delta f_2) \times P(\Delta f_3) \times [1 - P(\Delta f_4)] \times P(\Delta f_5) \times [1 - P(\Delta f_6)]$
A_{18}	$\Delta f_2 U \Delta f_3 U \Delta f_6$	$P(\Delta f_2) \times (\Delta f_3) \times [1 - P(\Delta f_4)] \times [1 - P(\Delta f_5)] \times P(\Delta f_6)$
A_{19}	$\Delta f_2 U \Delta f_4 U \Delta f_5$	$P(\Delta f_2) \times [1 - P(\Delta f_3)] \times P(\Delta f_4) \times P(\Delta f_5) \times [1 - P(\Delta f_6)]$
A_{20}	$\Delta f_2 U \Delta f_4 U \Delta f_6$	$P(\Delta f_2) \times [1 - P(\Delta f_3)] \times P(\Delta f_4) \times [1 - P(\Delta f_5)] \times P(\Delta f_6)$
A_{21}	$\Delta f_2 U \Delta f_5 U \Delta f_6$	$P(\Delta f_2) \times [1 - P(\Delta f_3)] \times [1 - P(\Delta f_4)] \times P(\Delta f_5) \times P(\Delta f_6)$
A_{22}	$\Delta f_3 U \Delta f_4 U \Delta f_5$	$[1 - P(\Delta f_2)] \times P(\Delta f_3) \times P(\Delta f_4) \times P(\Delta f_5) \times [1 - P(\Delta f_6)]$
A_{23}	$\Delta f_3 U \Delta f_4 U \Delta f_6$	$[1 - P(\Delta f_2)] \times P(\Delta f_3) \times P(\Delta f_4) \times [1 - P(\Delta f_5)] \times P(\Delta f_6)$
A_{24}	$\Delta f_2 U \Delta f_5 U \Delta f_6$	$[1 - P(\Delta f_2)] \times P(\Delta f_3) \times [1 - P(\Delta f_4)] \times P(\Delta f_5) \times P(\Delta f_6)$
A_{25}	$\Delta f_4 U \Delta f_5 U \Delta f_6$	$[1 - P(\Delta f_2)] \times [1 - P(\Delta f_3)] \times P(\Delta f_4) \times P(\Delta f_5) \times P(\Delta f_6)$
A_{26}	$\Delta f_2 U \Delta f_3 U \Delta f_4 U \Delta f_5$	$P(\Delta f_2) \times P(\Delta f_3) \times P(\Delta f_4) \times P(\Delta f_5) \times [1 - P(\Delta f_6)]$
A_{27}	$\Delta f_2 U \Delta f_3 U \Delta f_4 U \Delta f_6$	$P(\Delta f_2) \times P(\Delta f_3) \times P(\Delta f_4) \times [1 - P(\Delta f_5)] \times P(\Delta f_6)$
A_{28}	$\Delta f_2 U \Delta f_3 U \Delta f_5 U \Delta f_6$	$P(\Delta f_2) \times P(\Delta f_3) \times [1 - P(\Delta f_4)] \times P(\Delta f_5) \times P(\Delta f_6)$
A_{29}	$\Delta f_2 U \Delta f_4 U \Delta f_5 U \Delta f_6$	$P(\Delta f_2) \times [1 - P(\Delta f_3)] \times P(\Delta f_4) \times P(\Delta f_5) \times P(\Delta f_6)$
A_{30}	$\Delta f_3 U \Delta f_4 U \Delta f_5 U \Delta f_6$	$[1 - P(\Delta f_2)] \times P(\Delta f_3) \times P(\Delta f_4) \times P(\Delta f_5) \times P(\Delta f_6)$
A_{31}	$\Delta f_2 U \Delta f_3 U \Delta f_4 U \Delta f_5 U \Delta f_6$	$P(\Delta f_2) \times P(\Delta f_3) \times P(\Delta f_4) \times P(\Delta f_5) \times P(\Delta f_6)$

Таблица 3

Словесная разборчивость, рассчитанная по результатам артикуляционных испытаний

Обозначение сочетания A_j	Включаемые октавные полосы Δf_i	Вероятность распознавания слов $P(W\|A_j)$
A_0	$\varnothing$	0
A_1	Δf_2	0,006
A_2	Δf_3	0,082
A_3	Δf_4	0,149
A_4	$\Delta f5$	0,132
A_5	Δf_6	0,066
A_6	$\Delta f_2 U \Delta f_3$	0,302
A_7	$\Delta f_2 U \Delta f_4$	0,435
A_8	$\Delta f_2 U \Delta f_5$	0,527
A_9	$\Delta f_2 U \Delta f_6$	0,313
A_{10}	$\Delta f_3 U \Delta f_4$	0,448
A_{11}	$\Delta f_3 U \Delta f_5$	0,781
A_{12}	$\Delta f_3 U \Delta f_6$	0,692

Обозначение сочетания A_j	Включаемые октавные полосы Δf_i	Вероятность распознавания слов $P(W\|A_j)$
A_{13}	$\Delta f_4 U \Delta f_5$	0,781
A_{14}	$\Delta f_4 U \Delta f_6$	0,732
A_{15}	$\Delta f_5 U \Delta f_6$	0,675
A_{16}	$\Delta f_2 U \Delta f_3 U \Delta f_4$	0,668
A_{17}	$\Delta f_2 U \Delta f_3 U \Delta f_5$	0,864
A_{18}	$\Delta f_2 U \Delta f_3 U \Delta f_6$	0,811

Окончание табл. 3

Обозначение сочетания A_j	Включаемые октавные полосы Δf_i	Вероятность распознавания слов $P(W\|A_j)$
A_{19}	$\Delta f_2 U \Delta f_4 U \Delta f_5$	0,882
A_{20}	$\Delta f_2 U \Delta f_4 U \Delta f_6$	0,890
A_{21}	$\Delta f_2 U \Delta f_5 U \Delta f_6$	0,705
A_{22}	$\Delta f_3 U \Delta f_4 U \Delta f_5$	0,889
A_{23}	$\Delta f_3 U \Delta f_4 U \Delta f_6$	0,887
A_{24}	$\Delta f_2 U \Delta f_5 U \Delta f_6$	0,901
A_{25}	$\Delta f_4 U \Delta f_5 U \Delta f_6$	0,906
A_{26}	$\Delta f_2 U \Delta f_3 U \Delta f_4 U \Delta f_5$	0,934
A_{27}	$\Delta f_2 U \Delta f_3 U \Delta f_4 U \Delta f_6$	0,917
A_{28}	$\Delta f_2 U \Delta f_3 U \Delta f_5 U \Delta f_6$	0,926
A_{29}	$\Delta f_2 U \Delta f_4 U \Delta f_5 U \Delta f_6$	0,927
A_{30}	$\Delta f_3 U \Delta f_4 U \Delta f_5 U \Delta f_6$	0,940
A_{31}	$\Delta f_2 U \Delta f_3 U \Delta f_4 U \Delta f_5 U \Delta f_6$	1,000

С целью проверки достоверности расчетов по методике, в основу которой положен вероятностный метод, были проведены экспериментальные исследования словесной разборчивости речи методом артикуляционных испытаний.

При проведении экспериментальных исследований в качестве исходных тестовых речевых сигналов использовались две артикуляционные таблицы слов ГОСТ 16600-72 «Требования к разборчивости речи и методы артикуляционных измерений». Всего были получены аудиозаписи 100 слов.

Для формирования шумовых сигналов (в качестве шума использовался «белый» шум) и их смешения с исходными тестовыми речевыми сигналами использовалось специальное программное обеспечение Adobe Audition CC.

Для проведения экспериментальных исследований были получены аудиозаписи тестовых зашумленных сигналов при отношениях сигнал/шум от – 20 дБ до 0 дБ с шагом 2 дБ. Для каждой аудиозаписи было проведено измерение отношений сигнал/шум в октавных полосах.

В качестве аудиторов привлекались 18 человек (9 мужчин и 9 женщин). Все аудиторы не имели дефектов слуха.

Прослушивание аудиторами аудиозаписей зашумленных тестовых речевых сигналов осуществлялось через головные наушники, подключаемые к линейному выходу звуковой карты ПЭВМ, начиная с отношения сигнала/шум –20 дБ до отношения сигнал/шум 0 дБ с шагом 2 дБ.

После каждого прослушанного слова в специальное поле рабочего окна программы аудитор записывал слова, которые услышал. При невозможности разобрать слово поле оставлялось пустым.

После окончания тестирования программа автоматически рассчитывала среднее количество правильно распознанных слов (для всех слов и для всех аудиторов).

Проведенный анализ данных экспериментальных исследований показал, что зависимость словесной разборчивости речи от отношения сигнал/шум может быть аппроксимирована функцией:

$$W \approx \Phi(0{,}14 \cdot q - 1{,}33),$$

где W – словесная разборчивость речи;

q – интегральное отношение сигнал/шум, дБ.

Результаты сравнительной оценки результатов расчетов по методике, в основу которой положен вероятностный метод, с результатами артикуляционных испытаний приведены на рис. 1.

Анализ полученных графиков (рис. 1) показывает высокую сходимость результатов расчетов по методике, в основу которой положен вероятностный метод, с экспериментальными данными.

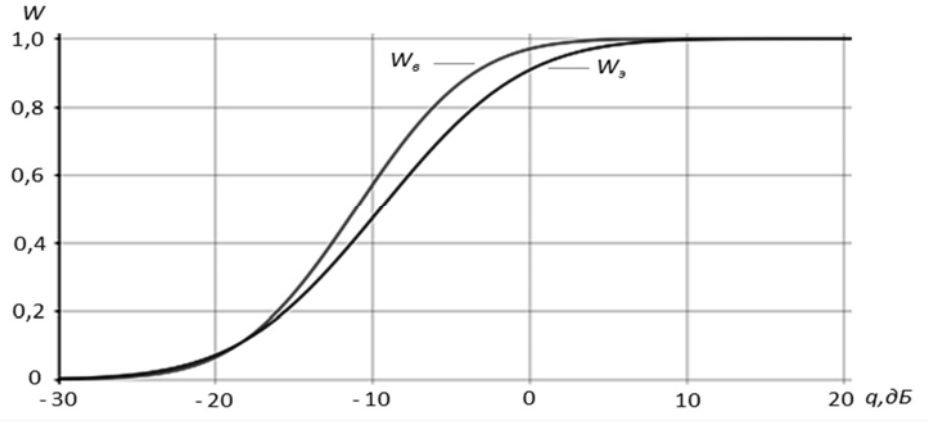


Рис.1. Графики зависимости словесной разборчивости речи (W) от отношения сигнал/шум (q), полученные по результатам расчетов по методике, в основу которой положен вероятностный метод ($W_в$), и по результатам артикуляционных испытаний ($W_э$)

Разница между рассчитанными и экспериментальными значениями возможно объясняется тем, что при проведении испытаний некоторые слова, включенные в артикуляционные таблицы, были труднораспознаваемыми, даже при высоких отношениях сигнал/шум, что повлияло на результаты испытаний.

Результаты сравнительной оценки результатов расчетов по методике, в основу которой положен вероятностный метод, с результатами расчетов по методике, в основу которой положен формантный метод, приведены на рис. 2.

Как видно из рис.2, словесная разборчивость речи, рассчитанная по методике, в основу которой положен вероятностный метод, выше, чем рассчитанная по методике, в основу которой положен формантный метод. Это может быть обусловлено тем, что в методике, в основу которой положен формантный метод, учитывается только тот случай, когда оператор услышит звуки речи во всех октавных полосах, а в методике, в основу которой положен вероятностный метод – во всех возможных комбинациях октавных полос, в которых оператор может услышать звуки речи.

Однако, словесная разборчивость речи, рассчитанная по методике, в основу которой положен формантный метод, несколько ниже, чем полученная по результатам экспериментальных исследований.

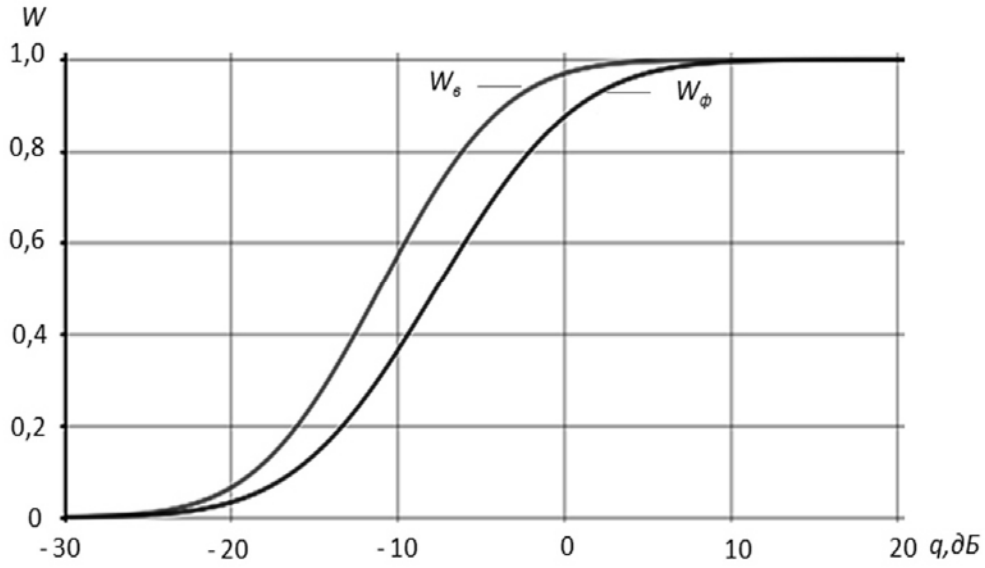


Рис. 2. Графики зависимости словесной разборчивости речи (W) от отношения сигнал/шум (q), полученные по результатам расчетов по методике, в основу которой положен вероятностный метод ($W_в$), с результатами расчетов по методике, в основу которой положен формантный метод ($W_ф$)

Учитывая, что при защите информации занижение возможностей средств акустической разведки противника может привести к утечке речевой информации, разработанная методика может быть использована для оценки эффективности защиты акустической речевой информации от ее утечки по техническим каналам, так как дает более высокие значения разборчивости речи, по сравнению с используемой в настоящее время методикой, в основу которой положен формантный метод.

Список литературы

1. Железняк, В. К. Некоторые методические подходы к оценке эффективности защиты речевой информации / В. К. Железняк, Ю. К. Макаров, А. А. Хорев // Специальная техника. – 2000. – № 4 – С. 39–45.

2. Хорев, А. А. Методика вероятностной оценки разборчивости речи / А. А. Хорев, И. С. Порсев // Защита информации. Инсайд. – 2020. – № 2 – С. 44–52.

УДК 577.3.043

ЭМОЦИОНАЛЬНОЕ СОСТОЯНИЕ ОПЕРАТОРА В УСЛОВИЯХ ЭЛЕКТРОМАГНИТНЫХ ШУМОВЫХ ИЗЛУЧЕНИЙ

А.В. СИДОРЕНКО, Н.А. СОЛОДУХО
Белорусский государственный университет, г. Минск, Республика Беларусь

Введение. Быстрое развитие информационных технологий, глобальной сети Интернет и социальных сетей привело к формированию информационной среды, оказывающей влияние практически на все сферы человеческой деятельности. Возникает необходимость развития методологических основ передачи информации, поиска системных решений с применением эффективных алгоритмов и методов построения средств защиты информации для обеспечения ее достоверности.

Особую остроту приобретает проблема обеспечения информационной безопасности, в том числе, предупреждения искажения информации, несанкционированного доступа, либо ее модификации. Для защиты информации от несанкционированного доступа по каналам электромагнитных излучений могут использоваться радиопоглощающие материалы и генераторы электромагнитного шума. Одним из показателей состояния центральной нервной системы является эмоциональное состояние. При этом предъявляются повышенные требования как к безопасности циркулирующей информации, так и к повышению защищенности человека от техногенных излучений, стрессов и других факторов воздействия. Существенное значение приобретают вопросы обеспечения стабильности эмоционального состояния человека, работающего в условиях необходимости принятия решений, в том числе, в мобильных (передвижных) системах.

На сегодняшний момент в литературе присутствуют противоречивые данные о влиянии электромагнитного излучения [1,2], в том числе и шумового [1, 3] на центральную нервную систему человека. Исследование же эмоционального состояния оператора под воздействием электромагнитных шумовых излучений, обработки и анализа паттернов электроэнцефалограмм (являющихся отражением функционального состояния центральной нервной системы) на основе хаотической динамики, фрактального анализа и моделей эмоционального состояния апредставляет несомненный интерес.

1. Методы анализа эмоционального состояния человека по электроэнцефалограммам. Эмоциональные состояния представляют собой психические состояния, которые возникают в процессе жизнедеятельности субъекта и определяют не только уровень информационно-энергетического обмена, но и направленность поведения.

Эмоциональное состояние человека может быть оценено таким количественными параметрами, как эмоциональная валентность и активность. Измеряемыми показателями, на основе которых определяется активность и эмоциональная валентность, являются: спектральная плотность мощности альфа-ритма электроэнцефалограмм в отведениях: *Fpz*, *F3*, *F4* и бета-ритма электроэнцефалограммы в отведениях: *Fpz*. Активность отображает степень расслабленности или возбуждения человека.

Активность А рассчитывается как отношение спектральной плотности мощности бета-ритма к спектральной плотности мощности альфа-ритма электроэнцефалограммы отведения *Fpz*

$$A = I_{Fpz\beta}/I_{Fpz\alpha},$$

где $I_{Fpz\beta}$ – спектральная плотность мощности альфа-ритма электроэнцефалограммы отведения *Fpz*;

$I_{Fpz\alpha}$ – спектральная плотность мощности альфа-ритма электроэнцефалограммы отведения *Fpz*.

Эмоциональная валентность отражает позитивность или негативность испытываемой эмоции. Чем больше эмоциональная валентность, тем приятнее испытываемая эмоция.

Эмоциональная валентность рассчитывается как отношение спектральной плотности мощности альфа-ритма электроэнцефалограммы отведения F3 к спектральной плотности мощности альфа-ритма электроэнцефалограммы отведения F4

$$V = I_{F3\alpha}/I_{F4\alpha},$$

где $I_{F3\alpha}$ – спектральная плотность мощности альфа-ритма электроэнцефалограммы отведения *F*4.

Возможна оценка эмоций, испытывает человек радость или злость, при использовании спектральной плотности мощности тета-, альфа-, бета-, гамма-ритмов электроэнцефалограмм в отведениях *Fp*1, *Fp*2, *F*3, *F*4, *P*3, *P*4, *T*3, *T*4.

Кроме перечисленных, существуют также способы интерпретации эмоций, например, на основе извлечения вызванных потенциалов; получаемые при множественном вейвлет-преобразовании; при эмпирическом разложении на моды; при использовании метода опорных векторов.

2. Методика проведения исследований. Регистрация электроэнцефалограмм осуществлялась по схеме «10/20» с использованием электроэнцефалографа «Нейрокартограф» фирмы МБН.

Обработка и анализ электроэнцефалограмм проводились в разработанной нами информационно-измерительной системе, адаптированной для работы с электроэнцефалограммами. Объектом исследований являлись электроэнцефалограммы следующих отведений: *Fp*1, *Fp*2, *F*3, *F*4, *P*3, *P*4, *T*3, *T*4, *Fpz*. Сигнал отведения *Fpz* был получен усреднением соответствующих значений сигналов отведений *Fp*1 и *Fp*2. Электроэнцефалограммы обрабатывались в следующих режимах: фон, наличие генератора шумового электромагнитного излучения. В фоне использовались электроэнцефалограммы здорового человека [3].

Спектральная плотность мощности ритмов головного мозга рассчитывалась с помощью быстрого преобразования Фурье. Анализируемые диапазоны ритмических составляющих включали: альфа-ритм (8–12) Гц, бета-ритм (12–20) Гц, тета-ритм (4–8) Гц, гамма-ритм (20–40) Гц.

3. Результаты и их обсуждение. Анализ вариаций спектральной плотности мощности тета-, альфа- бета-, гамма-ритмов электроэнцефалограмм проводились в отведениях: *Fp*1, *Fp*2, *F*3, *F*4, *P*3, *P*4, *T*3, *T*4. В фоновом режиме и режиме при наличии излучения наблюдается всплеск бета-ритма в электроэнцефалограммах теменной области (отведения *P*3 и *P*4), характерный для злости. Следует отметить, что при действии шумового излучения вспеск находится в электроэнцефалограмме отведения *P*3, а в фоновом режиме – в электроэнцефалограмме отведения *P*4, т. е. наблюдается сдвиг в левую теменную область головы по отношению к фону. При сравнении тета-ритма фонового режима и режима с излучением отмечено возрастание спектральной плотности мощности тетак-ритма в режиме электромагнитного шумового излучения. Такая же тенденция наблюдается для бета-, гамма- и альфа-ритмов. При сравнении спектральной плотности мощности гамма-ритма для радости и злости с аналогичным ритмом при наличии генерптора шума наблюдается картина, близкая к появлению радости, в отличие от фонового режима. Сравнительный анализ, проведенный по уровню спектральной плотности мощности тета- и альфа-ритмов при наличии генератора шума и в фоне, показывает наличие эмоции, характерной для злости.

При воздействии электромагнитного шумового излучения наблюдаемые изменения спектральной плотности мощности альфа-ритма сводятся к следующему. В отведении Fpz спектральная плотность мощности электроэнцефалограммы при наличии генератора шума увеличилась на 85,5 % относительно фона, в отведении *Fp*1 спектральная плотность мощности электроэнцефалограммы увеличилась более, чем в 3,5 раза относительно фона, в отведении *Fp*2 спектральная плотность мощности электроэнцефалограммы при действии излучения возросла на 21,0 % относительно фона. В отведении *F*3 спектральная плотность мощности электроэнцефалограммы выросла более, чем в 3,1 раза относительно фона, в отведении *F*4 прирост спектральной плотности мощности электроэнцефалограммы при наличии генератора шума составил 3,4 % относительно фона. В отведении *P*3 спектральная плотность мощности увеличилась почти в 3,4 раза относительно фона, в отведении *P*4 спектральная плотность мощности электроэнцефалограммы при наличии генератора шума снизилась на 23,1 %

относительно фона. В отведении *T*3 спектральная плотность мощности электроэнцефалограммы возросла более, чем в 7,1 раза относительно фона, в отведении *T*4 прирост спектральной плотности мощности электроэнцефалограммы при наличии генератора шума составил 42,3 % относительно фона. Возрастание альфа-ритма электроэнцефалограмм почти во всех отведениях может свидетельствовать об увеличении степени расслабленности человека и уменьшении зрительной активности под действием генератора шума.

Под влиянием электромагнитного шумового излучения происходят следующие изменения спектральной плотности мощности бета-ритма. В отведении *Fpz* спектральная плотность мощности анализируемого ритма электроэнцефалограммы при наличии шумового излучения возросла почти в 2,6 раза относительно фона; в отведении *Fp*1 спектральная плотность мощности ритма электроэнцефалограммы увеличилась более чем в пять раз относительно фона; в отведении *Fp*2 спектральная плотность мощности анализируемого ритма электроэнцефалограммы при наличии шумового сигнала возросла на 56,1 %. В отведении *P*3 спектральная плотность мощности бета-ритма увеличилась более чем в 3,5 раза относительно фона; отведении *P*4 значение спектральной плотности мощности бета-ритма электроэнцефалограммы при наличии генератора шумам снизилось на 16,7 % относительно фона. В отведении *T*3 анализируемый параметр электроэнцефалограммы вырос почти в 3,5 раза относительно фона; в отведении *T*4 прирост спектральной плотности мощности бета-ритма электроэнцефалограммы при наличии генератора шума составил 41,0 % относительно фона. Увеличение мощности бета-компонент электроэнцефалограммы в научной литературе рассматривается как один из показателей скрытой тревоги, расстройств, связанных с ней.

Рассмотренные выше вариации спектральной плотности мощности различных ритмов головного мозга позволили определить изменения эмоционального состояния. Как показал проведенный анализ серии опытов, значения эмоциональной валентности при воздействии электромагнитного шумового излучения увеличились более чем в три раза относительно фона, а активность выросла на 38,3 % относительно фона. Это является подтверждением положительных эмоций, свидетельствует о появлении возбуждения.

Заключение. Проведен комплекс экспериментальных исследований паттернов электроэнцефалограмм отведений *Fp*1, *Fp*2, *F*3, *F*4, *P*3, *P*4, *T*3, *T*4 при действии электромагнитного шумового излучения.

Изменение количественных параметров: эмоциональной валентности и активности показывают, что при действии электромагнитного шумового излучения оператор испытывает возбуждение, получает положительные эмоции. При сравнении спектральных плотностей мощности тета- и альфа-ритмов при действии на головной мозг электромагнитного шумового излучения и в фоне возникают эмоции в виде злости. Интерпретация полученных результатов основана на литературных источниках [4].

Предварительно полученные результаты об эмоциональном состоянии оператора при действии электромагнитных шумовых излучений свидетельствует о необходимости проведения в этом направлении дальнейших исследований.

Список литературы

1. Сидоренко, А. В. Показатели нелинейной динамики при наличии излучений мобильной связи и радиопоглощающих полиуретановых композитов / А. В. Сидоренко // Биомедицинская радиоэлектроника. – 2013. – № 12. – С. 44–52.

2. Павлова, Л. Н. Экспериментальная оценка реакций ЦНС на воздействие импульсных ЭМИ низкой интенсивности / Л. Н. Павлова, Л. П. Жаворонков, Б. В. Дубовик // Радиация и риск. – 2010. – № 3, т. 19. – С. 104–119.

3. Сидоренко, А. В. Нелинейный анализ электроэнцефалограмм оператора при действии электромагнитного шумового излучения / А. В. Сидоренко, Н. А. Солодухо // Доклады БГУИР. – 2017. – № 6. – С. 69–75. – 2014.

4. Francesca, M. M. Emotional valence and arousal affect reading in an interactive way: neuroimaging evidence for an approach-withdrawal framework / M.M. Francesca // Neuropsychologia. – 2014. – V. 56. – P. 79–89.

УДК 004.056

АНАЛИЗ МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ЗАЩИТЫ БАЗОВЫХ СИСТЕМ ВВОДА-ВЫВОДА СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

И.С. ГЕФНЕР, Ю.К. ЯЗОВ
Федеральное автономное учреждение
«Государственный научно-исследовательский испытательный институт
проблем технической защиты информации Федеральной службы
по техническому и экспортному контролю», Российская Федерация

В настоящее время задача обеспечения безопасного функционирования БСВВ является одним из наиболее актуальных в области защиты информации. Ввиду значимости функций, которые выполняет БСВВ для обеспечения работоспособности средств вычислительной техники, многие организации и специалисты в области защиты информации занялись исследованием вопросов, связанных с обеспечением безопасного функционирования БСВВ, а также разработкой комплекса мер и рекомендаций по организации ее защиты [1].

Для того чтобы определить дальнейшие направления деятельности в данной области, важно провести критический анализ мировой практики в области нормативного и методического обеспечения защиты БСВВ.

Как показал такой анализ, решение данной задачи представляет собой трудоемкий процесс, требующий описания структурно-функциональных характеристик БСВВ, ее взаимодействия со средствами вычислительной техники и анализом уязвимостей БСВВ. С этой целью организации и органы власти, занимающиеся вопросами информационной безопасности и информационных технологий, разрабатывают методические и нормативно-правовые документы, в которых отражены концептуальные подходы и организационно-технические рекомендации по организации защиты БСВВ.

Анализ зарубежного опыта показывает [2, 3], что значительное внимание вопросам защиты БСВВ уделяют в США. Национальным институтом стандартов и технологий США разработан ряд методических документов, содержащих рекомендации по защите БСВВ от угроз несанкционированного доступа.

Лаборатория информационных технологий Национального института стандартов и технологий содействует развитию сферы информационных технологий. Институт разрабатывает стандарты и руководящие документы для обеспечения защиты конфиденциальной информации и информации, обрабатываемой в государственных органах власти.

Одним из разработанных институтом стандартов является Руководство по безопасности базовых систем ввода-вывод для персональных компьютеров [3]. Стандарт разработан для федеральных органов исполнительной власти, частных организаций и разработчиков аппаратных платформ и БСВВ, а также специалистов в области информационной безопасности, ответственных за обеспечение защиты аппаратных модулей вычислительной системы и микропрограммного обеспечения.

В документе предусмотрены меры по предотвращению несанкционированного изменения микропрограммного обеспечения БСВВ на персональных компьютерах за счет вредоносного программного обеспечения.

Рекомендации по обеспечению безопасности БСВВ, определенные в документе, реализуются с помощью следующих процедур:

– аутентификации обновления БСВВ с использованием цифровых подписей для проверки подлинности новой прошивки;

– безопасного механизма локального обновления без цифровой подписи за счет непосредственного контроля со стороны администратора системы;

– защиты целостности прошивки для предотвращения ее изменения способом, который не соответствует двум вышеперечисленным;

– выполнения функций защиты, которые гарантируют отсутствие механизма, способного обойти защиту БСВВ.

В Руководстве по безопасности базовых систем ввода-вывод для персональных компьютеров приведена информация о принципах функционирования, роли БСВВ в процессе загрузки информационной системы, а также описан процесс загрузки БСВВ и современной версии БСВВ – унифицированного интерфейса расширяемой прошивки (УИРП).

Рекомендации по обеспечению безопасного функционирования БСВВ направлены на нейтрализацию следующих четырех угроз безопасности информации:

– несанкционированное обновление БСВВ посредством физического доступа к информационной системе;

– несанкционированная модификация БСВВ за счет наличия уязвимостей микропрограммного обеспечения БСВВ;

– внедрение вредоносного кода в микропрограммное обеспечение БСВВ сервера информационно-вычислительной сети, приводящее к заражению информационных систем, входящих в состав сети;

– использование уязвимой версии обновлений БСВВ.

Национальным институтом стандартов и технологий США разработаны новые правила безопасности БСВВ серверов (NIST 800-147B) [3]. Документ разработан по аналогии с рекомендациями по обеспечению безопасности БСВВ для персональных компьютеров. Меры защиты БСВВ серверов реализуются с помощью проверки подлинности обновления прошивки БСВВ, механизмов безопасного локального обновления, целостности прошивки, а также гарантий отсутствия способов по обходу системы защиты БСВВ.

Ввиду специфики серверных вычислительных архитектур, представленные в NIST 800-147 механизмы защиты БСВВ дополнены мерами по обеспечению безопасности обновления БСВВ. Это связано с наличием нескольких способов обновления БСВВ в серверных системах.

В стандарте NIST 800-147B представлены три способа защищенного обновления БСВВ:

1. Безопасное обновление БСВВ во время работы системы. Оно происходит на сервере во время работы системы, при этом не требуется перезагрузка и не нарушается ее работоспособности;

2. Безопасное обновление БСВВ при перезагрузке. С помощью данного механизма обновления БСВВ процесс обновления БСВВ запускается на сервере, а обновленная версия начинает работать только после перезагрузки сервера;

3. Безопасное обновление, при котором требуется подтверждение при загрузке. С помощью этого механизма обновления БСВВ происходит идентификация прошивки БСВВ с помощью цифровой подписи. В случае не подтверждения подлинности выполнение недостоверной БСВВ будет прекращено и запустится механизм возврата предшествующей прошивки.

Другим документом, регулирующим вопросы защиты БСВВ, является проект стандарта по измерению, оценке и контролю целостности БСВВ (NIST 800-155(Draft)) [4]. В стандарте определены способы обнаружения изменений кода и конфигурации БСВВ, связанных с нарушением конфиденциальности, целостности и доступности, включая нестабильность работы, отказ системы, утечку информации, а также компьютерные атаки. Данный стандарт описывает способы разработки безопасных механизмов оценки целостности БСВВ для разработчиков и производителей микропрограммного обеспечения.

Гарантией целостности БСВВ является корень доверия. Он реализует набор механизмов вычисления, хранения и передачи параметров достоверности БСВВ и ее конфигурации. Данные механизмы состоят из следующих составляющих:

– корень доверия оценки измерений, с помощью которого определяется достоверность результатов вычисления целостности;

– корень доверия системы хранения данных, применяемый для поддержания процесса вычисления параметров целостности и их последующего хранения;

– корень доверия создания отчетов, обеспечивающий механизмы сбора информации о процессах вычисления, хранения и передачи информации об измерениях целостности.

Кроме того, к системе контроля целостности относятся цифровая подпись БСВВ, механизмы обновления и виртуализация (если БСВВ выполняется на виртуальной машине).

Ввиду актуальности вопросов защиты БСВВ принят международный стандарт, содержащий требования к защите БСВВ (ISO/IEC 19678) [5]. Международный стандарт по информационной безопасности разработан Международной организацией по стандартизации и Международной электротехнической комиссией. Стандарт подготовлен Национальным институтом стандартов и технологий США по аналогии с NIST 800-147 и содержит организационно-технические требования к защите БСВВ. ISO/IEC 19678 устанавливает перечень угроз безопасности БСВВ и требования защиты БСВВ от несанкционированного доступа.

Анализ российских нормативных и методических документов по технической защите информации показал, что документы, регламентирующие деятельность по обеспечению безопасности БСВВ или иного микропрограммного обеспечения, отсутствуют.

При этом существует ряд документов, где отмечается необходимость защиты БСВВ, а также представлена информация об анализе уязвимостей и угроз безопасности информации данного компонента.

Федеральной службой по техническому и экспортному контролю (ФСТЭК России) в рамках деятельности по технической защите информации, разработан методический документ, описывающий процедуру моделирования угроз безопасности информации в информационных системах (Модель угроз) [6]. В Модели угроз описаны, в том числе, угрозы, при реализации которых объектом воздействия является БСВВ. В Модели угроз представлены исходные данные по объекту воздействия, способу реализации и степени ущерба от угроз несанкционированного доступа к защищаемой информации. Угрозы реализуются за счет получения доступа к информации и командам, хранящимся в БСВВ, что позволяет перехватить управление загрузкой операционной системы и получить права привилегированного пользователя.

Для моделирования угроз безопасности информации ФСТЭК России разработан банк данных угроз безопасности информации [7]. В обобщенном перечне угроз безопасности информации представлено 16 угроз, объектом воздействия которых является БСВВ. Угрозы безопасности информации связаны с несанкционированным доступом к БСВВ, внедрением вредоносного кода, установкой уязвимой версии БСВВ, использованием поддельных цифровых подписей, обходом механизмов защиты от записи в БСВВ.

Также ФСТЭК России разработаны Требования к средствам доверенной загрузки (Требования) [8]. Средства доверенной загрузки представляет собой программный или программно-технические средства, реализующие функции по предотвращению несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники на этапе его загрузки. Требования предназначены для организаций, разрабатывающих средства защиты информации, заявителей на осуществление обязательной сертификации продукции, а также для испытательных лабораторий и органов по сертификации. В них представлены три типа средств доверенной загрузки, к одному из которых относятся средства доверенной загрузки уровня БСВВ. Они направлены на нейтрализацию угроз безопасности информации, связанных с несанкционированным доступ к информации за счет загрузки нештатной операционной системы и обхода правил разграничения доступа операционной системы.

В настоящее время существует острая необходимость в дальнейшем совершенствовании нормативной базы в области защиты средств вычислительной техники на уровне БСВВ. Она заключается в определении подходов к разработке мер защиты в зависимости от того, какое место БСВВ занимает по отношению к объекту защиты. При этом с учетом проведенного анализа нормативных и методических документов целесообразно применить к БСВВ традиционный подход, разработанный ФСТЭК России применительно к построению систем защиты информации в информационных системах (рис. 1).

Для реализации указанного подхода необходимо выполнить следующие действия:

- определить объекты защиты БСВВ, представляющие собой совокупность взаимосвязанных компонентов, выполняющих заданные функции, каждый из которых может быть подвержен реализации угроз безопасности информации;

- определить нарушителей безопасности БСВВ, их возможности и способы реализации им угроз безопасности информации;

- определить условий реализации нарушителями угроз безопасности информации с учетом наличия физического или удаленного доступа к системе, наличия прав администратора, возможности изменять настройки БСВВ;

Рис. 1. Подход к построению системы защиты БСВВ

- оценить сценарии реализации угроз безопасности информации на объекты защиты БСВВ;

- реализовать механизмы защиты информации БСВВ с учетом определенных сценариев реализации угроз безопасности информации.

Изложенный подход к защите БСВВ позволит специалисту по защите информации сформировать модели безопасности БСВВ с учетом состава и содержания функций БСВВ, угроз безопасности информации и существующих мер по защите БСВВ.

Список литературы

1. Bulygin, Y. Summary of Attacks Against BIOS and Secure Boot. Available [Электронный ресурс] / Y. Bulygin [et al.]. – Режим доступа : Internet -http://www.infoworld.com.

2. BIOS Protection Guidelines. Recommendations of the National Institute of Standards and Technology. Special Publication 800-147 [Электронный ресурс]. – Режим доступа : http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147 April2011.pdf.

3. BIOS Protection Guidelines for Servers. Recommendations of the National Institute of Standards and Technology. Special Publication 800-147b. 2012 [Электронный ресурс]. – Режим доступа : http://csrc.nist.gov/publications /nistbul/itlbul2014_10.pdf (дата обращения 18.07.2016).

4.BIOS Integrity Measurement Guidelines. Recommendations of the National Institute of Standards and Technology (Draft). Special Publication 800-155. 2011 [Электронный ресурс]. – Режим доступа : http://csrc.nist.gov/publications/drafts/800-155/draft-SP800-155_Dec2011.pdf. – Дата доступа : 18.07.2016.

5.ISO/IEC 19678:2015 Information Technology – BIOS Protection Guidelines [Электронный ресурс]. – Режим доступа : https://www.iso.org/obp/ui/#iso:std:iso-iec:19678:ed-1:v1:en.

6.Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год (выписка) [Электронный ресурс]. – Режим доступа : http://fstec.ru/component/attachments/download/289.

7.Банк данных угроз безопасности информации [Электронный ресурс]. – Режим доступа : http://www.bdu.fstec.ru.

8. Об утверждении Требований к средствам доверенной загрузки : инф. Сообщение, 6 февраля 2014 г., № 240/24/405 [Электронный ресурс]. – Режим доступа : http://fstec.ru/component/attachments/download/663].

УДК 621.315.5

ЭЛАСТИЧНЫЕ МЕДЬСОДЕРЖАЩИЕ ЭЛЕКТРОМАГНИТНЫЕ ЭКРАНЫ ДЛЯ СНИЖЕНИЯ РАДИОЛОКАЦИОННОЙ ЗАМЕТНОСТИ НАЗЕМНЫХ ОБЪЕКТОВ

О.В. БОЙПРАВ, Н.В. БОГУШ, Л.М. ЛЫНЬКОВ, Е.С. БЕЛОУСОВА
Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

В работах [1, 2] представлены результаты исследований, направленных на установление закономерностей взаимодействия электромагнитного излучения (ЭМИ) в диапазоне частот 0,7…17,0 ГГц с изготовленными в соответствии со способом [3] эластичными электромагнитными экранами на основе фрагментов алюминиевой фольги и углеродосодержащих материалов в зависимости от состава, а также параметров геометрических неоднородностей поверхности таких экранов. На основе этих результатов установлено, что что указанные экраны характеризуются значениями коэффициента отражения ЭМИ в диапазоне частот 0,7…17,0 ГГц, достигающими величины –20,0 дБ (при условии выполнения измерений значений указанного параметра в режиме короткого замыкания) и значениями коэффициента передачи ЭМИ в обозначенном диапазоне частот, достигающими величины –40,0 дБ, в связи с чем могут быть использованы в целях снижения радиолокационной заметности наземных объектов. Низкие значения коэффициента отражения ЭМИ рассматриваемых экранов обусловлены тем, что их поверхность характеризуется наличием геометрических неоднородностей, размер которых сопоставим с длиной электромагнитных волн в обозначенном диапазоне частот, в связи с чем эти неоднородности обеспечивают рассеяние взаимодействующих с ними электромагнитных волн [4]. Низкие значения коэффициента передачи ЭМИ рассматриваемых экранов обусловлены тем, что в их состав входят материалы, характеризующиеся проводящими свойствами. Кроме того, изготовленные в соответствии со способом [3] эластичные электромагнитные экраны по сравнению аналогами, являются воздухопроницаемыми.

Исследование, результаты которого представлены в настоящем докладе, стало продолжением исследований, результаты которых представлены в работах [1, 2]. Его цель заключалась в установлении закономерностей взаимодействия ЭМИ в диапазоне частот 0,7…17,0 ГГц с эластичными медьсодержащими электромагнитными экранами, изготовленными в соответствии со способом [3], в зависимости от отношения суммарной площади поверхности фрагментов медьсодержащих листовых материалов, входящих в состав таких экранов, к площади поверхности последних (далее по тексту указанное отношение будет обозначаться с помощью символа «*k*»). Такая цель была поставлена на основе предположения о том, что изготовленные в соответствии со способом [3] эластичные медьсодержащие электромагнитные экраны будут характеризоваться более высокой эффективностью по сравнению с электромагнитными экранами, результаты исследования которых представлены в работах [1, 2], что связано с тем, что медьсодержащие материалы характеризуются большей электропроводностью по сравнению алюминий- и углеродосодержащими материалами.

Для достижения представленной цели были определены следующие задачи:

1) изготовление в соответствии со способом [3] экспериментальных образцов эластичных медьсодержащих электромагнитных экранов, отличающихся значением *k*;

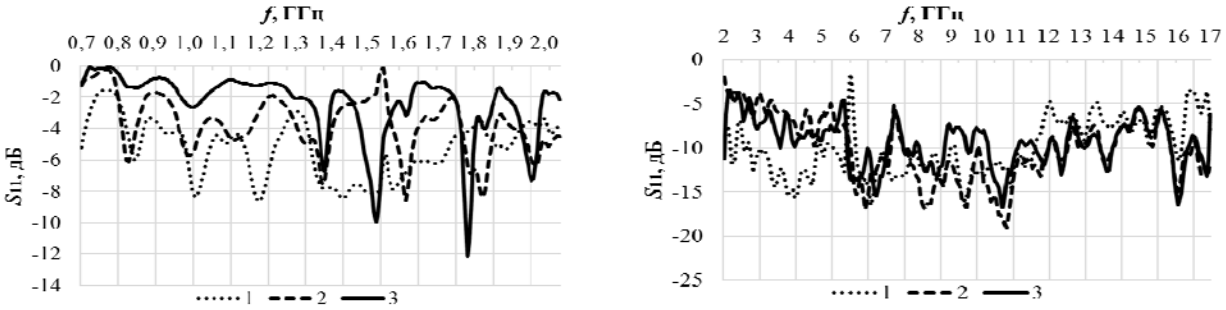
2) измерение значений коэффициентов отражения (режим согласованной нагрузки и режим короткого замыкания) и передачи ЭМИ в диапазоне частот 0,7…17,0 ГГц изготовленных экспериментальных образцов;

3) сравнительный анализ полученных на основе результатов измерений характеристик отражения и передачи ЭМИ в диапазоне частот 0,7…17,0 ГГц изготовленных экспериментальных образцов с аналогичными характеристиками, представленными в работах [1, 2].

В ходе решения первой из указанных задач в соответствии с методикой [3] были изготовлены три вида партий экспериментальных образцов эластичных электромагнитных экранов на основе фрагментов медьсодержащего листового материала, ширина которых составляла 0,5 ± 0,1 см, длина – 4,0 ± 0,2 см. Партия экспериментальных образцов первого вида (условное обозначение – партия образцов № 1) характеризовалась значением k, равным 0,7, партии экспериментальных образцов второго и третьего видов (условные обозначения – партии образцов № 2 и № 3 соответственно) – значениями k, равными 1,3 и 2,0 соответственно.

В ходе решения второй из указанных задач проводились измерения значений коэффициентов отражения и передачи ЭМИ изготовленных партий экспериментальных образцов с использованием панорамного измерителя коэффициентов отражения и передачи SNA 0.01–18 в соответствии с методикой, представленной в работе [5, с. 47].

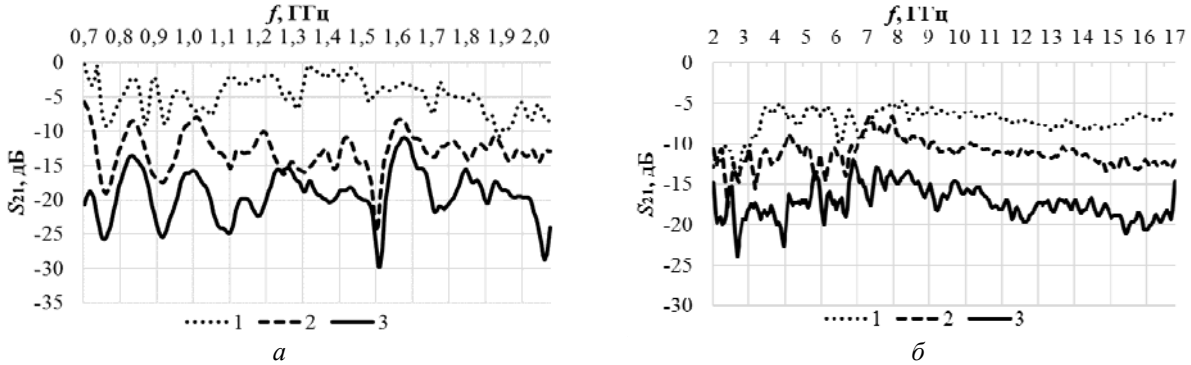
На рисунках 1 и 2 представлены частотные зависимости коэффициента отражения ЭМИ, полученные на основе результатов измерений, проведенных в режиме согласованной нагрузки, и частотные зависимости коэффициента передачи ЭМИ в диапазоне 0,7…17,0 ГГц изготовленных партий экспериментальных образцов.



а *б*

Рис. 1. Частотные зависимости коэффициента отражения ЭМИ в диапазоне 0,7…2,0 ГГц (*а*) и 2,0…17,0 ГГц (*б*) партий образцов № 1 (кривая 1), № 2 (кривая 2) и № 3 (кривая), полученные на основе результатов измерений, проведенных в режиме согласованной нагрузки

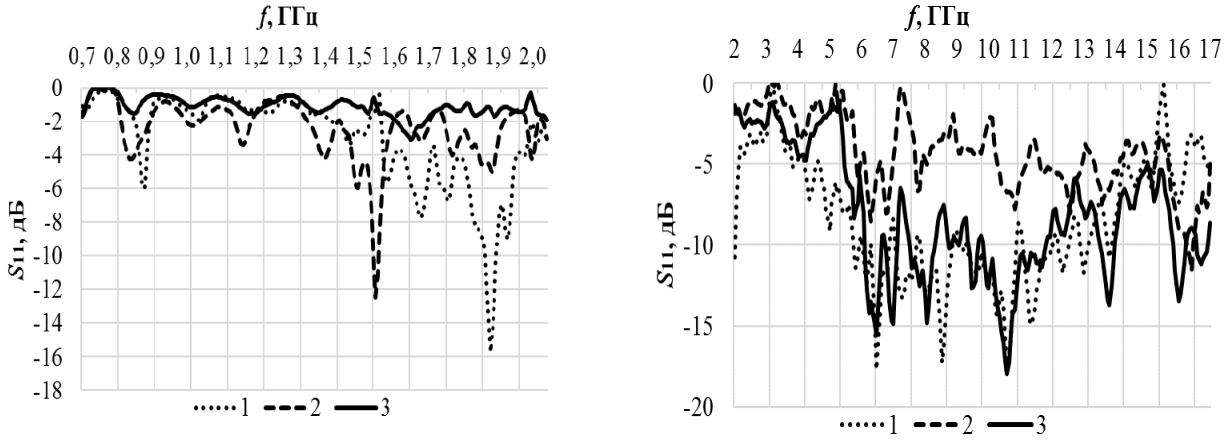
Из рисунков 1 и 2 следует, что значения коэффициентов отражения и передачи ЭМИ в диапазоне частот 0,7…17,0 ГГц эластичных медьсодержащих электромагнитных экранов изменяются в пределах от –2,0 до –15,0 дБ и от –1,0 до –10,0 дБ при условии, что для таких экранов характерно значение k, равное 0,7. Путем увеличения с 0,7 до 1,3 указанного значения можно обеспечить снижение на 5,0…20,0 дБ значений коэффициента отражения ЭМИ в диапазоне частот 0,7…17,0 ГГц рассматриваемых экранов при условии увеличения в среднем на 6,0 дБ значений их коэффициента отражения ЭМИ в диапазоне частот 0,7…6,0 ГГц. Если указанное значение, характерное для рассматриваемых электромагнитных экранов, увеличить с 1,3 до 2,0, то можно обеспечить снижение на 5,0…15,0 дБ значений их коэффициента передачи ЭМИ в диапазоне частот 0,7…17,0 ГГц и увеличение в среднем на 2,0 дБ значений их коэффициента отражения ЭМИ в диапазоне частот 0,7…2,0 ГГц. Снижение значений коэффициента передачи ЭМИ рассматриваемых электромагнитных экранов при увеличении значения k обусловлено увеличением их удельной проводимости.



а *б*

Рис. 2. Частотные зависимости коэффициента передачи ЭМИ в диапазоне 0,7…2,0 ГГц (*а*) и 2,0…17,0 ГГц (*б*) образцов № 1 (кривая 1), № 2 (кривая 2) и № 3 (кривая 3)

На рисунке 3 представлены частотные зависимости коэффициента отражения ЭМИ в диапазоне 0,7…17,0 ГГц исследованных образцов, полученные на основе результатов измерений, проведенных в режиме короткого замыкания.



а *б*

Рис. 3. Частотные зависимости коэффициента отражения ЭМИ в диапазоне 0,7…2,0 ГГц (*а*) и 2,0…17,0 ГГц (*б*) образцов № 1 (кривая 1), № 2 (кривая 2) и № 3 (кривая 3), полученные на основе результатов измерений, проведенных в режиме короткого замыкания

Из рисунка 3 следует, что измеренные в режиме короткого замыкания значения коэффициента отражения ЭМИ в диапазоне частот 0,7…17,0 ГГц рассматриваемых электромагнитных экранов изменяются в пределах от –2,0 до –16,0 дБ при условии, что для таких экранов характерно значение *k*, равное 0,7, в пределах от –2,0 до –16,0 дБ и от –2,0 до –17,0 дБ при условии, что для таких экранов характерно значение *k*, равное 1,3 и 2,0 соответственно.

На характеристиках отражения ЭМИ в диапазоне частот 0,7…2,0 ГГц рассматриваемых экранов имеются ярко выраженные минимумы. Наличие ярко выраженных минимумов на характеристиках отражения ЭМИ, представленных на рисунке 1, *а*, связано с тем, что электромагнитные волны, отражаемые от наружных поверхностей передних стенок рассматриваемых электромагнитных экранов, и электромагнитные волны, отражаемые от фрагментов медьсодержащего листового материала, образующих внутреннюю структуру таких экранов, и от внутренних поверхностей задних стенок последних, характеризуются большой разностью фаз на частотах, соответствующих минимальным значениям коэффициента отражения ЭМИ. Наличие ярко выраженных минимумов на характеристиках отражения ЭМИ, представленных на рисунке 2, *а*, связано с аналогичной особенностью с той лишь разницей, что она характерна не только для электромагнитных волн, отражаемых от наружных поверхностей передних и внутренних поверхностей задних стенок рассматриваемых электромагнитных экранов, но и для электромагнитных волн, отражаемых от поверхности металлической пластины, используемой в ходе проведения измерений в режиме короткого замыкания.

На основании полученных результатов измерений можно сделать следующие выводы:

1) по сравнению с электромагнитными экранами, результаты исследования которых представлены в работах [1, 2], исследованные электромагнитные экраны при условии, если соответствующее им значение *k* равно 2,0, характеризуются более высокой эффективностью экранирования в диапазоне частот 0,7…17,0 ГГц

2) по сравнению с электромагнитными экранами, результаты исследования которых представлены в работах [1, 2], исследованные электромагнитные экраны при условии, если соответствующее им значение *k* равно 0,7 характеризуются лучшими радиопоглощающими свойствами в диапазоне частот 0,7…17,0 ГГц.

Таким образом, предположение, на основании которого была поставлена цель исследования, подтвердилось.

Работа выполнена в рамках НИР «Эластичные и воздухопроницаемые электромагнитные экраны на основе фольгированных материалов для обеспечения информационной и экологической безопасности» по заданию № 1.5 «Разработка новых материалов и техноло-

гий для систем электромагнитной защиты радиоэлектронного и информационного оборудования, биологических объектов от воздействия широкого спектра электромагнитных излучений, обеспечения электромагнитной безопасности населения и электромагнитной совместимости электро-, радиотехнических средств и оборудования» ГПНИ «Материаловедение, новые материалы и технологии» на 2021–2025 гг.

Список литературы

1. Эластичные электромагнитные экраны на основе комбинированных металлосодержащих элементов / О. В. Бойправ [и др.] // Комплексная защита информации : мат-лы XXIII науч.-практ. конф., Суздаль, 22–24 мая 2018 г. – С. 312–315.

2. Электромагнитные экраны на основе трикотажных и фольгированных материалов для технических средств защиты информации / Л. М. Лыньков [и др.] // Комплексная защита информации : мат-лы XIX науч.-практ. конф. Витебск, 21–23 мая 2019 г. – С. 78–80.

3. Лыньков, Л.М. Способ изготовления эластичного электромагнитного экрана и электромагнитный экран, изготовленный этим способом / Л.М. Лыньков, В.А. Богуш, О.В. Бойправ // Патент Республики Беларусь № 23305. – Опубл. 28.02.2021.

4. Грудинская, Г. П. Распространение радиоволн / Г. П. Грудинская. – М. : Высшая школа, 1975. – 280 с.

5. Радиоэкранирующие модульные конструкции на основе порошкообразных материалов / Неамах Мустафа Рахим Неамах, [и др.] ; под ред. Л. М. Лынькова. – Минск : Бестпринт, 2013. – 182 с.

УДК 004.056

КОНТАКТНЫЙ ПЕРЕХВАТ В ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ МЕТОДОМ ОПТИЧЕСКОГО ТУННЕЛИРОВАНИЯ

В.В. ГРИШАЧЕВ
Российский государственный гуманитарный университет,
Институт информационных наук и технологий безопасности,
г. Москва, Российская Федерация

Введение. Численное моделирование перехвата информации на основе оптического туннелирования информационного сигнала из волоконно-оптического канала оптической системы связи в канал утечки показывает высокий уровень угроз информационной безопасности критической информационной инфраструктуры. Перехват может быть реализован скрытно в полевых условиях с вероятностью появления ошибочного бита, не большим чем в линии связи, даже при сохранении структуры оптического волокна и с минимальными разрушениями защитных оболочек кабеля.

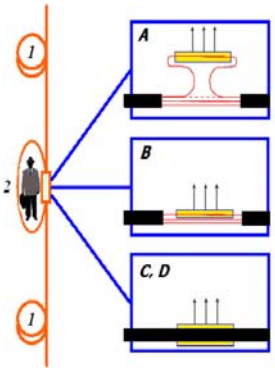
1. Проблема защиты информации в оптических сетях связи. В структуре современных систем связи определяющую роль играют оптические сети, в основе которых находятся волоконно-оптические системы передачи информации. Передача информации через оптический кабель дает значительные преимущества перед другими каналами связи, одно из которых высокая защищенность передачи от перехвата [1, 2]. Надо отметить, что повышенный уровень безопасности во многом определяется малой изученностью методов формирования каналов утечки и существует достаточно много технических решений получения доступа к передаваемой по волоконно-оптическим каналам информации.

Перехват информационного трафика в сетях связи – это несанкционированный доступ к передаваемой по сетям связи информации с помощью средств технической разведки, т. е. технических средств, не входящих в штатную инфраструктуру системы связи [2–5]. Структура перехвата включает штатный канал и линию связи, в котором формируется нештатный канал и линия утечки. Основой перехвата является физический способ подключения к штатному каналу связи. По способу подключения модель перехвата включает два вида (рис. 1):

– контактный перехват, формируемый путем отвода части информационного оптического сигнала из канала связи в канал утечки (рисунки 1*A*, 1*B*);

– дистанционный перехват, формируемый путем регистрации оптических и неоптических информативных сигнал без или с воздействием на канал связи (рисунки 1*C*, 1*D*).

Вид перехвата определяет используемые средства технической разведки и эффективность функционирования, т. е. уровень опасности угрозы.



КОНТАКТНЫЕ МЕТОДЫ:
A – контактный перехват с разрывом оптоволокна и вставкой;
B – контактный перехват с прямым доступом к волокну;
ДИСТАНЦИОННЫЕ МЕТОДЫ:
C – дистанционный перехват с регистрацией паразитных и сопутствующих излучений;
D – дистанционный перехват на основе параметрических методов

Рис. 1. Модель перехвата в оптических сетях: *1* – оптический кабель, *2* – нарушитель

1.1. Дистанционный перехват. Одно из главных преимуществ оптического канала по сравнению электрическими каналами связи состоит в отсутствии побочных электромагнитных излучений и наводок (ПЭМИН), но данное утверждение не является абсолютным. Как

показывают численное моделирование [6,7], в оптическом кабеле присутствуют информативные электромагнитные излучения на частотах близких к частотам модуляции информационного сигнала оптической несущей – паразитные электромагнитные излучения (ПрЭМИ), формируемые вследствие нелинейно-оптических преобразований, оценка мощности которых показывает возможность формирования дистанционного канала утечки. Также, в литературе обсуждается дистанционный перехват на основе ядерного магнитного резонанса и других физических явлений без проведения, какого-либо анализа. Все способы строятся на физических явлениях взаимодействия информационного сигнала с материалом канала связи, приводящее к информативным модуляциям параметров среды.

1.2. Контактный перехват. Отвод части излучения из оптоволокна является технической задачей требуемых для многих целей работы волоконно-оптических технологий, таких как объединение/разделение оптического потока в волокне, мультиплексирование/демультиплексирование и др. Данные технологии могут успешно применяться и в технике перехвата, тем более что некоторые устройства с подобными функциями применяются при монтаже и эксплуатации волоконно-оптических систем передачи информации. Например, в службах мониторинга сети используются устройства перехватчики трафика (network tap), которые представляются в виде включаемых в разрыв волокон с помощью штатных разъемов волоконно-оптического ответвителя и предназначенных для штатного контроля информационного трафика [1, 2]. Другое устройство, коммерческая волоконно-оптическая прищепка (например, FOD-5503) используется при монтаже и эксплуатации оптической сети для голосовой связи между монтажниками на расстояниях более 200 км, путем вывода/ввода части излучения на изгибе волокна [2].

Широкое распространение данных технических устройств, имеющих двойное назначение, привело к тому, что при анализе перехвата обсуждаются только эти два канала утечки. Их опасность значительно преувеличена, так как все они легко обнаруживаются службами мониторинга и безопасности либо при монтаже, либо при эксплуатации. Более или менее они эффективны для внутреннего нарушителя, который, используя свои знания работы локальной сети внутри охраняемого периметра, может подключить либо перехватчик трафика, либо прищепку-ответвитель. Перехват трафика в телекоммуникациях усложняется, так как разрыв канала будет обнаружен, отвод части информационного оптического сигнала на изгибе слишком значителен по величине, что скажется на функционале сети.

Анализ угроз показывает, что существуют другие более эффективные модели контактного перехвата, к которым относится перехват трафика на основе отвода части оптического излучения из канала связи в канал утечки путем оптического туннелирования [2, 3]. Хотя данный контактный перехват качественно описан достаточно давно, но физическое описание и оценки его эффективности отсутствуют. В данной работе данный пробел восполняется, что может позволить составить более полную модель угроз информационной безопасности трафику в оптических сетях.

2. Методика и оценка эффективности перехвата. Перехват трафика в информационных кабельных сетях имеет свои особенности и для их выявления необходимо определить технические характеристики формирования и функционирования канала утечки [2–5, 8–10]. Основными составляющими канала утечки являются способ физического доступа к информационному сигналу и формирования информативного сигнала, реализация канала утечки и технические средства регистрации. Кроме этого необходимо определиться с техническими характеристиками, определяющими эффективность функционирования канала утечки.

2.1. Каналы связи и утечки. Обобщенная структурная схема перехвата информационного трафика в оптических сетях представлена на рисунке 2. Штатная линия связи состоит из передатчика (1), канала связи (2) в виде оптического кабеля и приемника (3). Основными частями канала утечки являются система формирования информативного сигнала (4), например, путем отвода части излучения из канала связи в канал утечки, и система регистрации информативного сигнала (5). Функционирование канала утечки определяется методом формирования информативного сигнала, которое может быть реализовано различными способами.

Параметры линии связи определяются длиной канала ($\boldsymbol{L}$), мощностями оптического сигнала на входе ($\boldsymbol{P_{in}}$), т. е. мощностью передатчика, и на выходе ($\boldsymbol{P_{out}}$), т. е. на входе

в приемник, которые определяют бюджет линии связи (P_{in}–P_{out} в дБ). Величина P_{out} определяется чувствительностью приемника, которая не может быть выше этой величины. Также, на работу линии связи влияют шумовые характеристики линии, задаваемые отношениями сигнал/шум на входе SNR_{in} и выходе SNR_{out}, которые можно разделить на электронные в активных частях и оптические в канале связи.

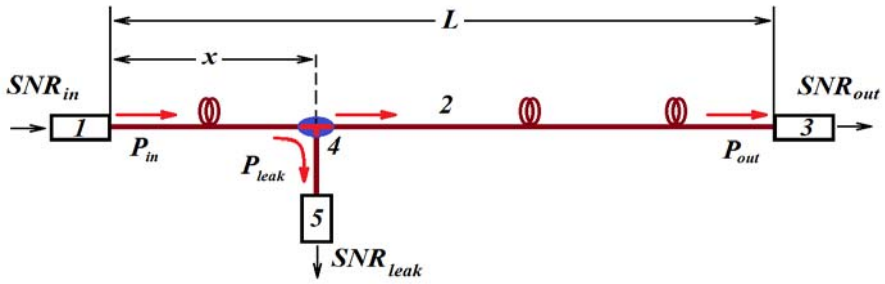


Рис. 2. Структурная схема перехвата трафика в оптических сетях:
1 – оптический передатчик линии связи с выходной мощностью P_{in} и отношением сигнал/шум SNR_{in}; *2* – волоконно-оптический канал связи длиной L; *3* – оптический приемник линии связи с входной мощностью P_{out} и отношением сигнал/шум SNR_{out}; *4* – система формирования информативного сигнала на расстоянии x от передатчика; *5* – канал утечки с оптическим приемником с отводимой мощностью P_{leak} и отношением сигнал/шум SNR_{leak}.

Параметры канала утечки определяются расстоянием (x) до места формирования информативного сигнала в канале утечки, выбор которого оказывает значительное влияние на его эффективность. Чем ближе к передатчику расположен отвод, тем выше мощность информационного сигнала и тем большую мощность с меньшими шумами информативного сигнала (P_{leak}) можно скрытно отвести от систем мониторинга. Эффективность перехвата во многом связана с шумами канала утечки SNR_{leak}, которые главным образом генерируются при подключении к штатному каналу связи и отводом в канал утечки. В других технических устройствах канала утечки шумы могут быть сокращены, путем использования малошумящих приемников и усилителей по сравнению со штатными устройствами линии связи, что позволит добиться лучших шумовых характеристик.

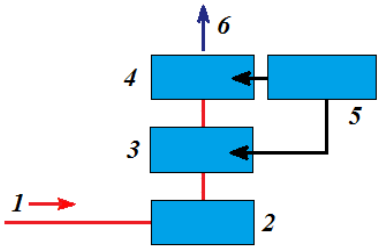


Рис. 3. Принципиальная блок-схема системы регистрации
в канале перехвата трафика:
1 – информативный оптический сигнал; *2* – оптический изолятор;
3 – оптический усилитель; *4* – приемный оптический модуль;
5 – источник питания; *6* – информативный электрический сигнал

Задача канала утечки состоит в перехвате информационного трафика в канале связи без потерь информации. В цифровых системах связи это связано с формированием канала утечки, в котором вероятность появления ошибочного бита (BER_{leak}) будет не больше, чем вероятность появления ошибочного бита (BER_{link}) в канале связи, т. е.

$$BER_{leak} \le BER_{link}.$$

Из этих предположений, если основными параметрами канала связи являются: (1) оптический бюджет линии P_{in}–P_{out}, с которым связана чувствительность приемника; (2) отношение сигнал/шум на входе SNR_{in} и на выходе SNR_{out} канала связи. Тогда, основными параметрами канала утечки, основанного на отведении части информационного оптического сигнала в канал утечки, является мощность P_{leak} и отношение сигнал/шум SNR_{leak} информативного оптического сигнала.

Ограничения на мощность отводимого информативного сигнала определяются: (1) чувствительностью оптического приемника канала утечки, который должен надежно регистрировать сигнал с вероятностью появления ошибочного бита не большим, чем в канале

связи; (2) с долей отводимой мощности из канала связи, которая должна быть такой малой, чтобы не быть обнаруженной системой мониторинга. На расстоянии x от передатчика мощность информативного сигнала $P_{leak} = P_x$ зависит от мощности информационного сигнала P_0 в месте формирования канала утечки, что позволяет ввести понятие коэффициента передачи мощности из канала связи в канал утечки

$$\kappa = \frac{P_x}{P_0}.$$

Дополнительные ограничения связаны с отношением сигнал/шум информативного сигнала – оно должно быть не меньше чем у штатного приемника канала связи. Для характеристики шумовых свойств каналов можно использовать понятие коэффициента шума элементов канала [8-10], т. е. отношение SNR на входе элемента к SNR на выходе соответствующего канала, так что интегральные коэффициенты шума канала связи и канала утечки определяются, соответственно, как

$$CNL_{link} = \frac{SNR_{in}}{SNR_{out}} \text{ и } CNL_{leak} = \frac{SNR_{in}}{SNR_{leak}}.$$

Каждый, из которых является произведением коэффициентов шума отдельных элементов, составляющих канал. Для канала утечки, его можно определить в виде произведения

$$CNL_{leak} = F_T \cdot F_L \cdot F_A \cdot F_R \approx F_T,$$

коэффициентов шума системы формирования информативного сигнала (F_T), линии передачи (F_L), усилителя (F_A) и преобразователя (приемника) (F_R). Наибольший вклад в зашумление информативного сигнала вносит система формирования информативного сигнала, что связано с необходимостью его создания в полевых условиях существующей линии связи, в то время как другие элементы могут быть изготовлены заранее промышленным способом с характеристиками, превосходящими штатные элементы.

Условием для достоверной оценки эффективности канала утечки является требование

$$CNL_{leak} \le CNL_{link},$$

тогда вероятность появления ошибочного бита в канале утечки будет не больше чем в канале связи, т. е. $BER_{leak} \le BER_{link}$.

Введенные параметры позволяют провести анализ эффективности функционирования каналов утечки на основе отвода части оптического излучения из канала связи и сделать предположения по эффективной защите линии связи от перехвата по отдельным типам. В частности, далее рассматривается канал утечки на основе отвода части оптического излучения из канала связи в канал утечки на основе оптического туннелирования.

3. Оптическое туннелирование в перехвате трафика. Явление оптического туннелирования состоит в нарушении полного внутреннего отражения на границе сердцевина/оболочка оптического волокна, которое связано с формированием поверхностной волны, проникающей внутрь оболочки с экспоненциально убывающей интенсивностью по глубине проникновения, варьирующуюся с углом падения и длиной волны [2, 3, 11–13]. Проникающая в оболочку отражаемая волна уходит от границы на расстояния нескольких длин волн и может быть захвачена другим волноводом. При условии фазового синхронизма в основном волноводе и дополнительном волноводе, перехватывающем часть поверхностной волны, происходит перетекание энергии волны, которое может быть полным.

3.1. Модель отвода оптической мощности из одного волновода в другой близко расположенный волновод представлена на рисунке 4. Два волноводных канала вдоль оси y шириной w с показателями преломления n_1 и n_2 разделены расстоянием s с показателем преломления n_3, образующим оптический контакт вдоль волокон длиной z по оси z. По информационному каналу связи распространяется оптическое информационное излучение мощностью P_0, в области оптического контакта часть излучения мощностью P_x переходит в информативный канал утечки.

Коэффициент передачи из канала связи в канал утечки для случая оптического туннелирования можно определить методом связанных мод [11-13] как

$$\kappa = \frac{K^2}{K^2 + (\Delta\beta/2)^2} \sin^2\left[\left(K^2 + (\Delta\beta/2)^2\right)^{1/2} z\right] \exp(-\alpha z),$$

который зависит от коэффициента связи оптических мод (***K***) в каналах связи и утечки, длиной оптического контакта волноводов z с оптическими потерями в канале связи $\boldsymbol{\alpha}$ и разностью постоянных распространения между ними $\boldsymbol{\Delta\beta}$.

В приближении малого поглощения ($\boldsymbol{\alpha} \ll \boldsymbol{1}$) и одинаковости волноводов ($\boldsymbol{\Delta\beta} \approx \boldsymbol{0}$) получим:

$$\kappa = \sin^2 Kz\,.$$

Отвод мощности из канала связи в канал утечки не должен быть большим. Он не должен превышать типичные значения потерь на оптических неоднородностях типа сварки (менее 0,1 дБ, порядка 0,01 – 0,02 дБ), поэтому отводимая мощность всегда много меньше 1 при $Kz < 0{,}1$, что позволяет определить коэффициент передачи в виде

$$\kappa = (Kz)^2\,.$$

Как видно, значение коэффициента передачи κ определяется коэффициентом связи K между волноводами каналов связи и утечки, а длина оптического контакта волноводов z играет роль параметра, с помощью которого можно влиять на величину коэффициента передачи.

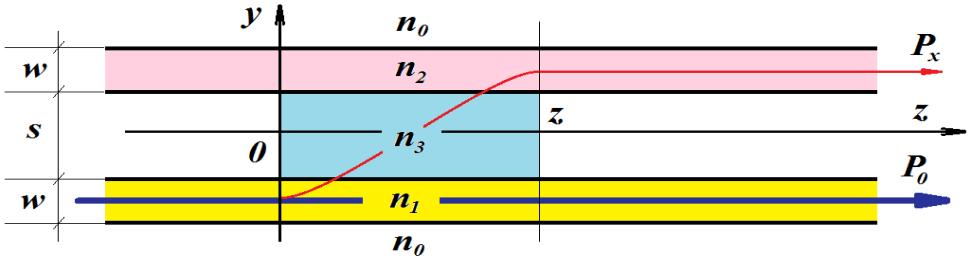


Рис. 4. Модель формирования информативного сигнала переходом части оптического информативного сигнала из волновода канала связи в волновод канала утечки путем оптического туннелирования: $\boldsymbol{n_0}$, $\boldsymbol{n_1}$, $\boldsymbol{n_2}$, $\boldsymbol{n_3}$ – показатели преломления окружающей среды, материала волноводов и среды оптического контакта волноводов, $\boldsymbol{w}$ – ширина (плоских) волноводов каналов связи и утечки, $\boldsymbol{s}$ – ширина среды оптического контакта, z – длина среды оптического контакта, $\boldsymbol{P_0}$ – мощность информационного оптического сигнала в канале связи, $\boldsymbol{P_x}$ – мощность информативного оптического сигнала в канале утечки

3.2. Оценка интегрального коэффициента передачи из канала связи в канал утечки может быть проведена в приближении плоских волноводов с параболическим профилем показателя преломления методом связанных мод. Для оценки используем геометрические и оптические параметры волноводов, близкие по величине к цилиндрическим волокнам оптических систем связи [1, 2].

Геометрические параметры: ширина волновода порядка диаметра сердцевины волокна – 8–9 мкм ($\boldsymbol{w/\lambda = 8}$), ширина оптического контакта меньше или порядка толщины оболочки волокна – ~60 мкм при диаметре оболочки 125 мкм ($\boldsymbol{s/\lambda \le 50}$).

Длина оптического контакта порядка 1 см ($\boldsymbol{z/\lambda = 10^4}$) выбирается из условий технической возможности фиксации протяженного контакта механическими и клеевыми приспособлениями, а также из условия фазового синхронизма связанных мод. Длина когерентности информационного оптического сигнала ограничивается частотой модуляции, следовательно, для скорости передачи информации более 10 ГГц длина когерентности составит порядка 6 см.

Оптические параметры: показатели преломления волноводов как у сердцевин выпускаемых оптоволокон порядка $\boldsymbol{n_1 = n_2 = 1{,}45}$, показатель преломления оптического контакта $\boldsymbol{n_3 = 1{,}44}$ (т. е. $\boldsymbol{n_1(n_2) - n_3 = 0{,}01}$) и критический угол $\boldsymbol{\theta_c = 1{,}45328}$ рад ($\sin\theta_c = n_3/n_2 = 0{,}9931$), т. е. пределы изменения угла падения $\theta \in \{\theta_c = 1{,}45328 \div 1{,}57080 = \pi/2\}$ и синуса угла падения $\sin\theta \in \{0{,}993103 \div 1\}$.

Предлагаемые приближения можно транслировать на цилиндрические волокна с определенными ограничениями, но они позволяют определить основные параметры оптического туннелирования по порядку величины, что вполне достаточно для поставленной задачи, по оценке эффективности канала утечки.

Коэффициент связи оптических мод ***K*** зависит от типа волноводов, расстояния между волноводами (***s***), длины (частоты) волны информационного сигнала (**ω** или **λ**), постоянной распространения волновода ($\beta = nk_0 \sin\theta$), показателя преломления среды волновода (***n***), волнового числа информационного сигнала в вакууме ($k_0 = 2\pi/\lambda$), угла падения (**θ**, принимающего значения от критического угла падения $\theta_c = \arcsin\left(n_3/n_1\right)$ до направления распространения вдоль оси волновода ***π/2***). В приближении плоских одинаковых волноводов с $\boldsymbol{n_1 = n_2}$, $\boldsymbol{\Delta\beta = 0}$ и параболическим профилем показателя преломления, коэффициент связи [11] имеет вид

$$K = -\frac{2\pi n_2\left(n_2^2\sin^2\theta - n_3^3\right)}{\lambda\left(n_2^3 - n_3^2\right)\left[1 + \pi\left(w/\lambda\right)\sqrt{n_2^2\sin^2\theta - n_3^3}\right]\sin\theta}\exp\left\{-2\pi\sqrt{n_2^2\sin^2\theta - n_3^3}\,\left(s/\lambda\right)\right\}.$$

Тогда коэффициент передачи может быть представлен в удобном для численного моделирования виде

$$\kappa = A\left(\frac{z}{\lambda}\right)^2\left[\frac{x^2}{\left[1 + B\left(w/\lambda\right)x\right]\sin\theta}\right]^2\exp\left\{-4B\left(\frac{s}{\lambda}\right)x\right\},$$

где введены безразмерные константы на основании принятых геометрических и оптических характеристик волноводов:

$$A = \frac{4\pi^2 n_2^6}{\left(n_2^3 - n_3^2\right)^2} = 4{,}4\cdot 10^5;\ B = \pi n_2 = 4{,}6;\ x = \sqrt{\sin^2\theta - \sin^2\theta_c}\ ;\ \sin^2\theta_c = \left(n_3/n_2\right)^2 = 0{,}986254$$

для n_2=1,45 и n_3= 1,44, λ=1,6 мкм, $\left(w/\lambda\right)$= 5, $\left(s/\lambda\right)$= 40, $\left(z/\lambda\right)$= 100.

В результате численного моделирования получена зависимость коэффициента передачи от угла падения $\kappa\left(\theta\right)$, которая имеет ярко выраженный максимум (рис. 5). Коэффициент передачи равен 0 при критических углах падения, с увеличением угла падения он быстро растет и достигает своего максимума. Приближение направления распространения к приосевым лучам приводит к быстрому падению коэффициента передачи до 0. Таким образом, коэффициент передачи имеет узкий по углу падения максимум, в котором сосредоточена небольшая доля мощности информационного сигнала. Величина максимума достигает 1 при увеличении длины оптического контакта более 1 мм. Это позволяет полностью отводить в канал утечки малые доли информационного потока, отклоняющиеся от приосевого направления распространения, что трудно фиксируется системами мониторинга сети.

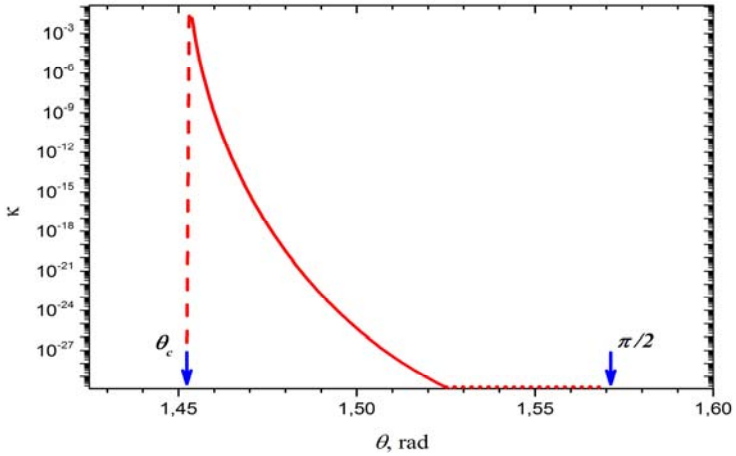


Рис. 5. Зависимость коэффициента передачи ***κ*** от угла падения **θ** в пределах от критического угла падения (**θ*c***) до прямого угла падения для показателей преломления одинаковых волноводов 1,45 и оптического контакта между ними 1,44, при ширине волноводов ***w/λ* = 5**, ширине оптического контакта ***s/λ* = 40**, длине оптического контакта ***z/λ* = 100**

Из графика зависимости к(θ) видно, что присутствующие в структуре потока направления лучей распространения близкие к критическому углу падения $\boldsymbol{\theta_c}$ будут эффективно переходить из канала связи в канал утечки. В приближении оптического контакта длиной по-

рядка ста длин волн (~160 мкм) и при ширине около 40 длин волн (~65 мкм) в канал утечки будет переходить более 1 % мощности всех лучей с углом падения близким к критическому углу. Увеличение длины оптического контакта в 100 раз до 16 мм приведет к вовлечению в процесс формирования информативного сигнала более удаленные от критического угла лучи со 100 % передачей в канал утечки. Более близкие к критическому углу лучи не будут оказывать существенного влияние на коэффициент передачи из-за нарушения волнового синхронизма между каналами. Таким образом, 100% передача будет происходить в узком диапазоне углов падения, ограниченных шириной диапазона углов с максимальной передачей, порядка 0,003 рад из общего диапазона углов порядка 0,1 рад. Интегральный коэффициент передачи мощности можно оценить в 1%. Такой вид зависимости $\kappa(\theta)$ предполагает возможность формирования регистрируемого информативного сигнала в канале утечки даже для цилиндрических волокон соединенных оптическим клеем без стравливания оболочки волокна до сердцевины, что значительно упрощает технику отвода светового потока и делает ее скрытной для мониторинга.

3.3. Оценка расстояния от передатчика линии связи до места перехвата. Мощность $\boldsymbol{P_{leak}}$ информативного сигнала в месте перехвата определяется исходной мощностью $\boldsymbol{P_{in}}$ передатчика, потерями $\boldsymbol{\alpha}$ в канале связи и коэффициентом передачи $\boldsymbol{\kappa}$, так что

$$P_{leak} = \kappa P_{in} \cdot 10^{-\alpha x}.$$

Минимальную отводимую в канал утечки мощность можно оценить в 10 фотонов на один бит, которая ограничивается шумами средств технической разведки канала утечки. Ограничение по мощности для скорости передачи информации 100 Гб/сек составит $P_{leak} < -40$ дБм (0,1 мкВт), отсюда получаем максимальную дальность перехвата

$$x < \frac{\lg\left(P_{in}/P_{leak}\right) + \lg\left(\kappa\right)}{\alpha}.$$

Для интегрального коэффициента передачи $\boldsymbol{\kappa}$ = 1%, мощности передатчика $\boldsymbol{P_{in}}$ = 10 дБм и потерей в канале связи $\boldsymbol{\alpha}$ = 0,5 дБ/км расстояние, до которого будет возможен перехват с принятой техникой разведки, достигнет 60 км.

3.4. Шумы информативного сигнала в канале утечки. При формировании информативного сигнала путем оптического туннелирования коэффициент связи оптических мод ($\boldsymbol{K}$) испытывает флуктуации вследствие теплового изменения расстояния между каналами ($\boldsymbol{\delta s}$), ширины спектра информационного сигнала ($\boldsymbol{\delta\omega}$), направления распространения ($\boldsymbol{\delta\theta}$), что вызывает флуктуации коэффициента передачи и, следовательно, искажения информативного сигнала в канале утечки, т. е. появление мультипликативных шумов. Аддитивными шумами можно пренебречь, так как проникновение из внешней среды или внутренние генерации света незначительны. В месте отвода оптического излучения среднеквадратичная мощность информационного сигнала в канале связи и информативного сигнала в канале утечки

$$P_x = S_x + N_x \text{ и } P_{leak} = S_l + N_l,$$

где первые слагаемые S_x и S_l мощности полезной части сигнала, а вторые слагаемые N_x и N_l мощности шумов. Среднеквадратичная мощность полезной части информативного сигнала

$$S_l = \kappa S_x - \delta\kappa S_x$$

и шумовой части

$$N_l = \delta\kappa S_x + \kappa N_x + N_a,$$

где $\delta\kappa$ – паразитные флуктуации коэффициента передачи, которые уменьшают величину полезной части информативного сигнала на $\delta\kappa S_x$ и на столько же увеличивают ее шумовую часть, $N_a = 0$ – аддитивные шумы, которыми пренебрегаем. Отсюда можно получить связь

отношения сигнал/шум информационного SNR_x и информативного SNR_{leak} сигналов в виде коэффициента шума канала утечки

$$CNL_{leak} = \frac{SNR_x}{SNR_{leak}} = \frac{1 + SNR_x\left(\delta\kappa/\kappa\right)}{1 - \left(\delta\kappa/\kappa\right)} \approx F_T .$$

Т. е. предполагается основной вклад в шумы дает способ формирования отвода части информационного сигнала из канала связи в канал утечки, шумы других частей канала утечки нивелируются выбором малошумящих средств технической разведки.

3.5. Оценка флуктуаций коэффициента передачи $\delta\kappa/k$ определяется относительными флуктуациями параметров оптического туннелирования, таких как угол падения ($\delta\theta/\theta$), ширина ($\delta s/s$) и длина ($\delta z/z$) оптического контакта, ширины волновода ($\delta w/w$) и других, связанных с тепловыми колебаниями в месте контакта. В приближении малости коэффициента передачи его величина связывается с относительными флуктуациями в принятых обозначениях и приближениях как

$$\frac{\delta\kappa}{\kappa} \approx 2\frac{\delta\left(Kz\right)}{Kz} \approx 2\sqrt{\left[\frac{\delta z}{z}\right]^2 + \left(\frac{Bx\left(w/\lambda\right)}{1 + Bx\left(w/\lambda\right)}\right)^2\left[\frac{\delta w}{w}\right]^2 + 16(Bx)^2\left[\frac{s}{\lambda}\right]^2\left[\frac{\delta s}{s}\right]^2} .$$

Учитывая большую длину оптического контакта и стабильность ширины волновода, коэффициент передачи можно оценить приближением

$$\frac{\delta\kappa}{\kappa} \approx 8\pi n_2\sqrt{\sin^2\theta - \sin^2\theta_c}\,\frac{\delta s}{\lambda} \approx 0{,}5.$$

Оценка коэффициента шума передачи

$$CNL_{leak} \approx F_T \approx 10 \text{ для } SNR_x = 8, \text{ т. е. } SNR_{leak} = 1.$$

Это значительно затрудняет перехват, но использование менее шумящего приемника по сравнению со штатным приемником линии связи можно достичь эффективного перехвата, т. е. С вероятностью появления ошибочного бита не большего штатной линии связи.

4. Особенности перехвата трафика в оптических сетях связи. Практическая реализация перехвата возможна при создании эффективного и стабильного оптического контакта между каналами связи, и утечки, что требует выполнения определенных условий по доступу к оптическому кабелю и технических решений по формированию отвода части оптического излучения.

На основе проведенного качественного анализа формирования информативного сигнала методом оптического туннелирования можно предложить несколько структурных схем реализации канала утечки (рис. 6). Несмотря на то, что значения коэффициента передачи должны быть малы, но, даже в этом случае, реализовать туннелирование света через защитные оболочки трудно из-за возрастания потерь и шумов. Поэтому, во-первых, необходимо освободить волокно от всех защитных оболочек до оптической оболочки волокна, составляющей в диаметре 125 мкм; во-вторых, в области оптического контакта с волокном канала связи необходимо использовать канал утечки в виде волновода без оболочки удобной формы, переходящее в обычное цилиндрическое волокно.

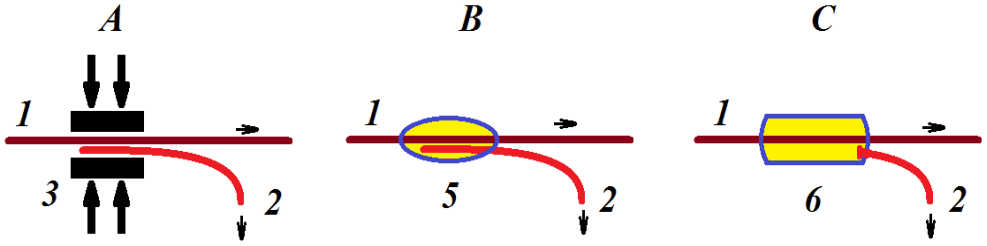


Рис. 6. Структурные схемы формирования в оптическом канале (*1*) оптического информативного сигнала (*2*) методом оптического туннелирования: *A* – путем плотного механического сжатия волокон (3), *B* – путем склеивания оптическим клеем волокон (*5*), *C* – путем наплава оптического клея в виде капли (*6*)

Формирование устойчивого оптического контакта можно осуществить механическим (рис. 6, *A*) или клеевым (рис. 6, *B*) способами без изгиба волокна. Последний способ предпочтительнее, так как более устойчив к внешним воздействиям – границы оптического клея выполняют фокусирующие функции для туннелирующего в него света и защитные функции от внешних воздействий, которые могут повлиять как на канал утечки, так и на канал связи. Дополнительное небольшое воздействие внешних физических полей на оптический контакт, в том числе и механическое воздействие (т. е. изгиб), может увеличить коэффициент передачи. Еще один способ (рис. 6, *C*) связан с использованием оптического клея как второй оболочки вокруг первой оболочки оптического волокна канала связи, в которую туннелирует свет и фокусируется на вход волокна канала утечки с градиентной линзой на конце.

Предложенные схемы позволяют реализовать перехват в полевых условиях простейшими средствами технической разведки с минимальными затратами по времени. В частности, формирование контакта с применением оптического клея можно реализовать без полного разрушения защитных оболочек кабеля, путем ввода клея и волокна канала утечки через малый прокол в кабеле полой цилиндрической трубкой на подобии иглы медицинского шприца.

Заключение. Проведенный анализ показывает высокий уровень угрозы сценария перехвата посредством отвода части оптического информационного сигнала из канала связи в канал утечки методом оптического туннелирования, противодействие которому требует разработки методов защиты кабельной системы, использования оптоволокна высокого качества, непрерывного мониторинга состояния канала связи и других действий. В существующих условиях эксплуатации волоконно-оптических систем передачи информации основным способов предотвращения перехвата является использование качественного оптического кабеля при качественном монтаже, которое позволяет уменьшить вероятность скрытного подключения.

Список литературы

1. Фриман, Р. Волоконно-оптические системы связи / Р. Фриман ; под ред. Н. Н. Слепова. – М. : Техно-сфера, 2007. – 511 с.

2. Шубин, В. В. Информационная безопасность волоконно-оптических систем / В. В. Шубин. – Саров : РФЯЦ-ВНИИЭФ, 2015. – 257 с.

3. Гришачев, В. В. Анализ каналов утечки информации в волоконно-оптических линиях связи: нарушение полного внутреннего отражения / В. В. Гришачев, В. Н. Кабашкин, А. Д. Фролов // Информационное противодействие угрозам терроризма. – 2005. – № 4. – С. 194 –204.

4. Булавкин, И. А. Вопросы информационной безопасности сетей PON / И. А. Булавкин // Технологии и средства связи. – 2006. – № 2. – С. 104–108.

5. Глущенко, А. Оценка защищенности информации, циркулирующей в ВОЛП / А. Глущенко, Л. Глущенко, В. Тупота // Фотоника. – № 4. – С. 36–42.

6. Гришачев, В. В. Анализ каналов утечки информации в волоконно-оптических линиях связи: пара-зитные электромагнитные излучения / В. В. Гришачев // Комплексная защита информации : мат-лы XXIV науч.-практ. конф. Витебск, 21–23 мая 2019 г. – Витебск : ВГТУ, 2019. С. 44–52.

7. Гришачев, В. В. Перехват трафика в оптических сетях: информативные паразитные электромагнитные излучения / В. В. Гришачев // Фотоника. – 2019. – Т. 13, № 3. – С. 280–294.

8. Гришачев, В. В. Количественная оценка эффективности канала утечки информации по техническим параметрам каналов связи / В. В. Гришачев, О. А. Косенко // Вопросы защиты информации. – 2010. – № 4. – С. 9–17.

9. Гришачев, В. В. Оценка коэффициента шума технического канала утечки информации / В. В. Гришачев, О. А. Косенко // Вопросы защиты информации. – 2011. – № 1. – С. 29–36.

10. Гришачев, В. В. Методика оценки параметров технического канала утечки информации / В. В. Гришачев // Вопросы защиты информации. – 2012. – № 1. – С. 12–16.

11. Сомех, С. Оптические ответвители / С. Сомех // Введение в интегральную оптику / С. Сомех ; под ред. М. Барноски. – М. : Мир, 1977. – С. 194–226.

12. Маркузе, Д. Связь между диэлектрическими волноводами Оптические волноводы / Д. Маркузе ; пер. С англ. – М. : Мир, 1974. – С. 519–549.

13. Снайдер, А. Теория оптических волноводов / А. Снайдер, Дж. Лав. – М. : Радио и связь, 1987. – С. 458–495.

УДК 621.391.16; 681. 327.8

ОЦЕНКА ЗАЩИЩЕННОСТИ РЕЧЕВЫХ СИГНАЛОВ ПРИ ДИСКРЕТНО-КВАНТОВАННОМ ПРЕОБРАЗОВАНИИ

М.М. БАРАНОВСКИЙ[1], А.Г. ФИЛИППОВИЧ[1], В.К. ЖЕЛЕЗНЯК[2], С.В. ЛАВРОВ[2]
[1]Оперативно-аналитический центр при Президенте Республики Беларусь, г. Минск, 220030, Республика Беларусь,
[2]Учреждение образования «Полоцкий государственный университет», г. Новополоцк, 211440, Республика Беларусь

Введение. Аналого-цифровые и цифро-аналоговые преобразователи повсеместно используются во всем современном оборудовании ввиду превосходства цифровой обработки сигналов над аналоговой. Преобразование аналоговых речевых сигналов в цифровые и их обратное преобразование из цифровой формы в исходный сигнал генерируют новые каналы утечки речевой информации. Установлено, что дискретизация по времени и квантование по уровню высокоскоростных высококачественных речевых сигналов при преобразовании их в цифровую форму являются основными источниками утечки информации [1].

Используемые в настоящее время подходы к оценке защищенности каналов утечки речевых сигналов при их преобразовании в цифровую форму сводятся к раздельной оценке аналогово речевого сигнала и речевого сигнала, представленного в цифровой форме при его передаче по линиям связи, а в качестве измерительного сигнала используют, как правило, гармонический сигнал [2, 3].

В работе [1] показано, что использование гармонического сигнала не позволяет достоверно оценить защищенность речевого сигнала при высококачественной скоростной передаче в цифровых системах информации, а при выборе измерительных (тестовых) сигналов необходимо учитывать особенности дискретно-квантованного представления речевых сигналов.

Задачей настоящей работы является повышение достоверности и точности оценки преобразованного дискретно-квантованного речевого сигнала за счет повышения точности оценки шума квантования.

1. Особенности дискретно-квантованного преобразования речевых сигналов. Защищенность речевого сигнала дискретно-квантованным равномерным преобразованием при амплитудно-импульсной модуляции оценивают по шуму квантования, используя амплитудную характеристику квантования [4]. Амплитудная характеристика квантования является ступенчатой функцией с равномерной величиной шага квантования Δ. Величина шага квантования определяется весом младшего числового разряда.

При равномерном квантовании с числом уровней квантования $L = 2^N$ (где N – число бит цифровой передачи) величину шага квантования Δ определяют по формуле:

$$\Delta = \frac{U_{\max}}{2}, \tag{1}$$

где $U_{\max}$ – общий динамический диапазон входного сигнала.

На рисунке 1, *а* приведена амплитудная характеристика квантования.

Разницу между входным аналоговым сигналом $x(t)$ и квантованным сигналом $y(t)$ называют ошибкой или шумом квантования $e(t)$:

$$e(t) = y(t) - x(t). \tag{2}$$

При этом $-\frac{\Delta}{2} \le e(t) \le \frac{\Delta}{2}$.

На рисунке 1, *б* представлена ошибка квантования для амплитудной характеристики квантования, изображенной на рисунке 1 (а). Из формулы (2) и рисунка 1 следует, что сигнал ошибки квантования зависит от амплитуды входного сигнала $x(t)$ и амплитудной характеристики квантования.

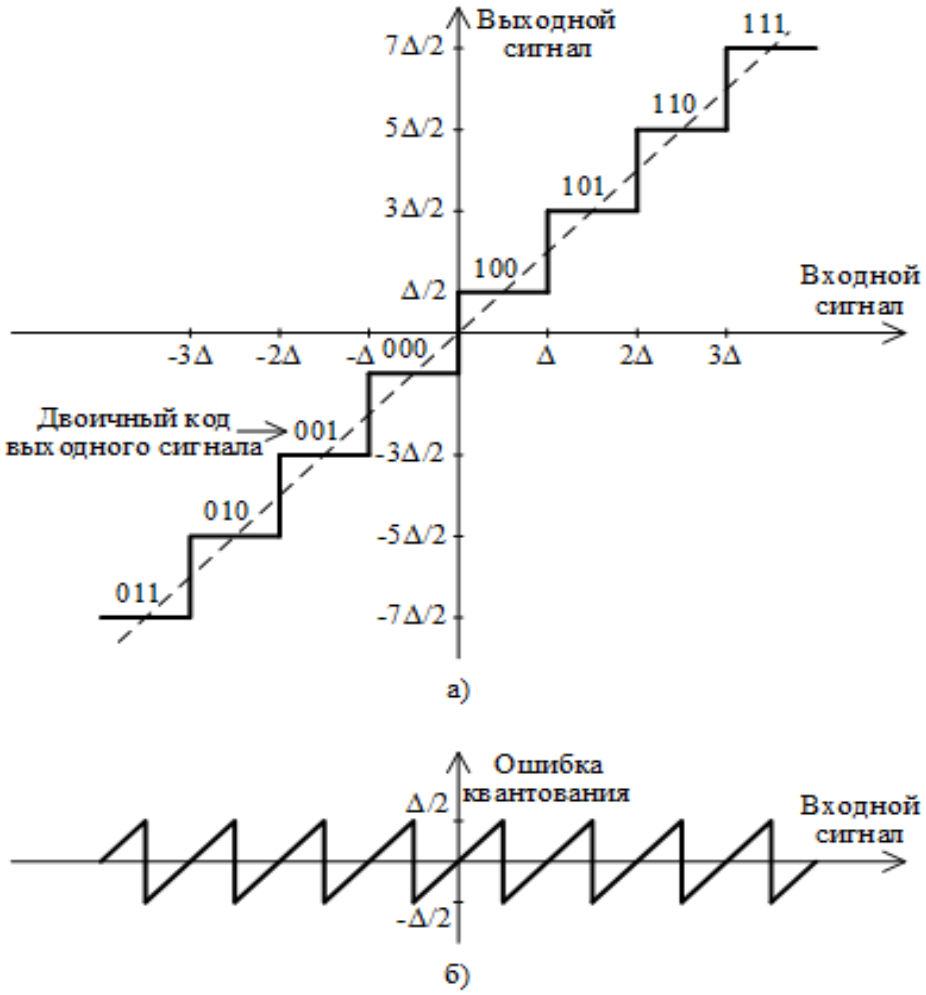


Рис. 1. Амплитудная характеристика квантования (*а*) и соответствующая ей ошибка квантования (*б*)

При одинаковых интервалах квантования среднее значение мощности ошибки квантования P_Δ и эффективное значение ошибки квантования ε_Δ зависят только от величины шага квантования [4]:

$$P_\Delta = \frac{\Delta^2}{12} = \frac{1}{12}\left(\frac{U_{\max}}{2^N}\right)^2, \tag{3}$$

$$\varepsilon_\Delta = \frac{\Delta}{2\sqrt{3}} = \frac{1}{\sqrt{3}}\left(\frac{U_{\max}}{2^{N+1}}\right). \tag{4}$$

В рабочей полосе частот ограниченной верхней полосы f_B отношение сигнал/шум (*SNR*) при равномерном квантовании зависит от длины кодовых слов N (бит) и частоты дискретизации Fд следующим образом [4]:

$$SNR = 6,02N + 101g\left(\frac{F_д}{2\Delta f_B}\right) + C_s, \tag{5}$$

где C_s – постоянная, учитывающая форму входного сигнала (для гармонических сигналов C_s = 1,7 дБ, для звуковых сигналов C_s = –15… +2 дБ).

Из формулы (5) видно, что при каждом удвоении частоты дискретизации Fд отношение сигнал/шум улучшается на 3 дБ. Для обеспечения заданного качества воспроизведения переданного сообщения требуется полоса 10 кГц и длина кодового слова должны быть не менее 12 бит [4].

Процесс дискретизации можно представить как умножение исходного сигнала $x(t)$ на решетчатую функцию $\delta_T^*(t)$, состоящую из периодической последовательности дельта функций, следующих с периодом T:

$$\delta_T^*(t) = \sum_{m=-\infty}^{\infty} \delta(t - mT). \quad (6)$$

Представление ее в виде ряда Фурье имеет следующий вид [5]:

$$\delta_T^*(t) = \frac{2\pi}{\omega_0} \sum_{k=-\infty}^{\infty} e^{jk\omega_0 t}, \quad (7)$$

где $\omega_0 = 2\pi/T$ – частота дискретизации, T – период (шаг) дискретизации;

Выходная величина $x^*(t)$ представляется модулированной последовательностью δ-функцией [5]:

$$x^*(t) = x(t) \cdot \delta_T^*(t) = \sum_{m=-\infty}^{\infty} x(t) \cdot \delta(t - mT) = \sum_{m=-\infty}^{\infty} x(mT) \cdot \delta(t - mT), \quad (8)$$

где $x(t) = x(mT)$ – решетчатая функция (последовательность дискретных значений непрерывной функции $x(t)$ при $0 \le mT < \infty$).

На рисунке 2 представлена полученная в соответствии с формулой (8) модулированная последовательность δ-функций $x^*(t)$.

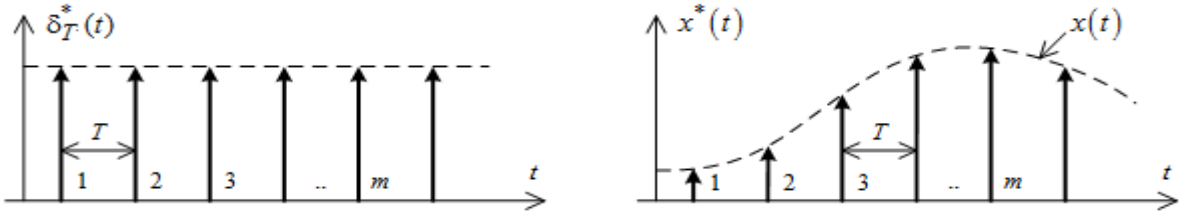


Рис. 2. Модулированная последовательность δ-функций

Формула (8) решает задачу восстановления сигнала по его значениям в точках отсчета, представленных с помощью сигнала δ-функций. Если входная непрерывная величина $x(t)$ обладает финитным свойством, т. е. спектр ограничен частотой среза ω_c, то квантование по времени с частотой $\omega_0 \ge 2\omega_c$ не приводит к потере информации. Для восстановления входного сигнала $x(t)$ необходимо на вход идеального фильтра нижних частот подать сигнал $x^*(t)$. Тогда на выходе фильтра нижних частот получим восстановленный сигнал [5]:

$$x(t) = \sum_{m=-\infty}^{\infty} x(mT) \frac{\sin \omega_c (t - mT)}{\omega_c (t - mT)}. \quad (9)$$

Формула (9) обосновывает замену передачи непрерывного сигнала передачей решетчатым сигналом без потери информации.

Кроме того, необходимо отметить, что использование гармонического сигнала не позволяет достоверно оценить защищенность речевых сигналов при дискретно-квантованном преобразовании в связи с:

- высокой погрешность оценки отношения уровня дискретизированного речевого сигнала к уровню шума квантования из-за того, что и сигнал, и шум квантования – случайные процессы;

- низкой точность и достоверность оценки защищенности, обусловленной искажением сигнала шума квантования из-за высокого по сравнению с его уровнем шума в точке наблюдения;

- отсутствием нормативного значения оценки защищенности речевого сигнала, преобразованного квантованно-дискретным преобразованием для передачи в широкополосных каналах.

2. Оценка защищенности дискретно-квантованного речевого сигнала. Для оценки защищенности речевых сигналов при дискретно-квантованном преобразовании предложено использовать в качестве измерительного сигнала периодическую импульсную последовательность треугольной формы, формируемую из периодической последовательности прямоугольных импульсов путем последовательного автокорреляционного преобразования [1]. Измерительному сигналу присуща форма линейно-нарастающего и линейно-спадающего напряжения с высокоточной линейностью. Высокая точность измерительного сигнала подтверждается сравнением амплитуд основной и высшей нечетных гармоник спектра периодической функции треугольной формы разложением в ряд Фурье в тригонометрическом виде [6]:

$$f(t)=\frac{8A}{\pi^2}\sum_{k=1}^{\infty}(-1)^{\frac{k-1}{2}}\frac{\sin k\omega t}{k^2}, \qquad (10)$$

где a – амплитуда сигнала; k – номер гармоники (k=1,3,5,…); $\omega=\frac{2\pi}{T_{\text{П}}}$ – угловая частота сигнала; $T_{\text{П}}$ – период сигнала.

Из формулы (10) видно, что для периодической импульсной последовательности треугольной формы четные гармоники отсутствуют, а амплитуды нечетных гармоник убывают пропорционально второй степени номеров гармоник, что позволяет производить оценку защищенности по первой (основной) гармонике. Возникающий при этом шум квантования имеет пилообразную форму, что повышает чувствительность его обнаружения.

Разложение импульсов пилообразной формы шума квантования в ряд Фурье имеет следующий вид [6]:

$$f\left(t\right)=\frac{A}{2}-\frac{A}{\pi}\sum_{k=1}^{\infty}\frac{1}{k}\sin k\omega t, \qquad (11)$$

где k = 1, 2, 3, …

Для формирования измерительного сигнала, в качестве исходного (нормированного) сигнала используем периодическую импульсную последовательность прямоугольной формы с периодом T, равным $1/F_i$, где F_i – средняя частота полосы, равной разборчивости речевого сигнала, $i=\overline{1,n}$, n = 20 [1], длительность импульса $\tau = T/2$, F_i = 250; 500; 650; 800; 950; 1125; 1300; 1500; 1700; 1875; 2050; 2250; 2425; 2725; 3100; 3500; 3850; 4550; 6150; 8600 Гц.

Преобразуем автокорреляционной функцией периодическую импульсную последовательность прямоугольной формы в периодическую импульсную последовательность треугольной формы. В результате преобразования получим необходимый измерительный сигнал, представленный в виде периодической импульсной последовательности треугольной формы с мощностью $A^2\tau$ и длительностью импульса 2τ [1], где A – амплитуда импульса импульсной последовательности прямоугольной формы и τ = 1000; 769; 625; 526; 444; 385; 333; 294; 267; 243; 222; 206; 183; 161; 143; 130; 110; 81; 58 мкс (рис. 3).

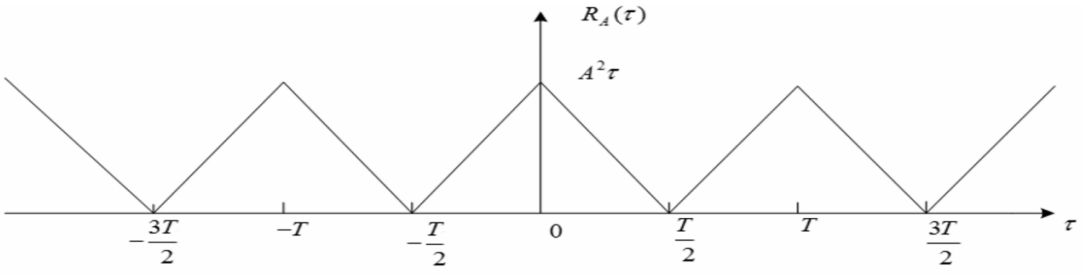


Рис. 3. Автокорреляционная функция

Полученный сигнал периодической импульсной последовательности треугольной формы без его искажения вводят в канал передачи речевого сигнала. На выходе канала передачи получают преобразованный сигнал в виде выборки и ошибки квантования, которые обрабатывают в каждой из полос равной разборчивости. Из периодической импульсной последовательности треугольной формы выделяют спектральные составляющие методом преобразования Фурье с получением основной гармоники гармонического сигнала. Для увеличения отношения сигнал/шум применяют накопление, при котором основная и высшие гармоники сигнала накапливаются по линейному закону, а шум – по среднеквадратичному. Оценку защищенности речевого сигнала выполняют сравнением полученного отношения сигнал/шум с нормированным [1].

Заключение. Для оценки защищенности канала утечки речевых сигналов при дискретно-квантованном преобразовании предложено использование измерительного сигнала треугольной формы. Предложен способ синтеза измерительного композитного сигнала, представленного в виде периодической импульсной последовательности треугольной формы, формируемой из периодической последовательности прямоугольных импульсов путем последовательного автокорреляционного преобразования. Использование предложенного измерительного композитного сигнала позволяет установить его численную зависимость с численным значением сигнала, принятого в качестве нормированного и сравнить для принятия решения о защищенности речевого сигнала. Полученные результаты позволяют проводить дальнейшие исследования защищенности речевых сигналов при их обратном преобразовании из цифровой формы в исходный сигнал.

Список литературы

1. Железняк, В. К. Синтез измерительного композитного сигнала для оценки защищенности речевых сигналов при дискретно-квантованном преобразовании / В. К. Железняк [и др.] // Доклады БГУИР. – 2020. – № 18 (6). – С. 81–87.

2. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам / Г. А. Бузов. – М. : Горячая линия – Телеком, 2017. – 586 с.

3. Железняк, В. К. Защита информации от утечки по техническим каналам : учеб. пособие / В. К. Железняк. – СПб.: ГУАП, 2006. – 188 с.

4. Шкритек, П. Справочное руководство по звуковой схемотехнике / П. Шкритек. – М. : Мир, 1991 – 446 с.

5. Цыпкин, Я. З. Основы теории автоматических систем / Я. З. Цыпкин. – М. : Наука, 1977. – 560 с.

6. Скляр, Б. Цифровая связь: теоретические основы и практическое применение / Б. Скляр [и др.] ; пер. с англ.. – 2-е изд. – М. [и др.] : Вильямс, 2016. — 1099 с.

УДК 004.46

КОНТРОЛЬ ПРОГРАММНО-АППАРАТНОЙ СРЕДЫ РАБОЧИХ МЕСТ ПОЛЬЗОВАТЕЛЯ

А.Ю. ЧАДОВ, Н.В. МОЗОЛИНА
Национальный исследовательский университет «Московский физико-технический институт», Российская Федерация

Введение. Контроль состояния и конфигурации информационной системы необходимо обеспечивать на этапах жизненного цикла с внедрения до утилизации [1].

В прошлом году на одной из секций конференции в докладе «Предъявите документы, или к вопросу о контроле изменений на рабочих местах пользователей» был представлен продукт ОКБ САПР «Паспорт ПО», позволяющий решить задачу контроля состояния программной среды рабочего места пользователя. На данный момент этот продукт внедрен в эксплуатацию в крупной территориально распределенной организации (десятки территориальных подразделений по всей стране) мы занимаемся его поддержкой и развитием, в процессе которых собираем отзывы и предложения от пользователей и постепенно улучшаем продукт.

О развитии «Паспорта ПО» и пойдет речь в текущем докладе.

1. Состав, функционирование и развитие «Паспорт ПО». Прежде чем перейти к направлениям доработок продукта, напомню из чего состоит и как функционирует «Паспорт ПО».

Основными элементами программного модуля (ПМ) «Паспорт ПО» являются:

1. Серверный компонент (Сервер) с базой данных;
2. Компонент управления (АРМ управления);
3. Клиентский компонент (Клиент), устанавливаемый на подконтрольные объекты (ПКО), – рабочие места (СВТ), конфигурацию которых контролирует программный модуль;
4. Сервис обмена сообщениями RabbitMQ, обеспечивающий взаимодействие по сети между всеми элементами [2].

Подготовка системы для работы ПМ «Паспорт ПО» заключается в выполнении следующих действий:

1. Регистрация учетных записей административного персонала, отвечающего за контроль целостности программной среды в АРМ управления, формирование ролей и назначение их учетным записям;
2. Формирование списка ПКО с разбиением на логические группы (подразделения);
3. Формирование общей базы шаблонов (прототипов конфигураций рабочих мест пользователей);
4. Назначение шаблонов подконтрольным объектам;
5. Проведение опроса на ПКО (сканирования конфигурации СВТ в соответствии с назначенным шаблоном) и формирование его паспорта ПО, то есть его эталонного состояния [3].

Паспорт СВТ представляет собой подписанный набор данных: различные данные о ПКО, включая имя и адрес в сети, данные о подписавшем паспорт сотруднике и время создания паспорта, данные о контролируемых файлах, включая полный путь и хэш-сумму, вычисленную от его содержимого, и данные о программах, установленных на подконтрольный объект.

В ходе дальнейшей работы программного модуля выполняется сканирование подконтрольных объектов по заданному для СВТ расписанию или по запросу управляющего персонала ПМ «Паспорт ПО». В ходе сканирования Клиент определяет конфигурацию программной среды СВТ и отправляет информацию на Сервер, который автоматически сверяет полученные данные о текущем состоянии ПКО с эталонным и информирует управляющий персонал ПМ «Паспорт ПО» о выявленных нарушениях. Для каждого ПКО в случае обнаружения нарушений управляющим персоналом должен быть выполнен анализ возникших изменений, в результате которого возможно обновление паспорта ПКО (в случае если это были санкционированные модификации) или же принятие мер по устранению причин возникших несоответствий, разбор инцидента безопасности [3].

Полученное в результате сканирования ПКО описание конфигурации СВТ называется «проект паспорта» или просто «проект». Такой проект для каждого ПКО в каждый момент времени существует только один, каждый новый проект автоматически заменяет предыдущий и таким образом всегда отражает последнее известное состояние СВТ.

За время эксплуатации были обнаружены возможности развития в нескольких разных направлениях и были предложены следующий доработки:

1. Возможность сохранения промежуточных проектов
2. Возможность контроля рабочих, работающих под управлением ОС семейства Linux.
3. Возможность контроля аппаратных средств рабочей станции

2. Сохранение промежуточных проектов. От одного из пользователей спустя некоторое время эксплуатации «Паспорта ПО» поступила просьба добавить возможность сохранения всех промежуточных проектов для того, чтобы информация обо всех промежуточных состояниях СВТ также была доступна для анализа в случае необходимости.

Это несложная доработка, требующая внесения небольших изменений в логику работы сервера и в АРМ управления. При появлении нового проекта старый будет не удаляться, а переводиться в состояние «архивный проект» и оставаться в БД. Но просто хранить проекты было бы недостаточно, ведь цель доработки – не просто добавить возможность просматривать промежуточные состояния СВТ, а полноценно следить за всеми изменениями (то есть за разницей между состояниями, отличиях от утвержденных паспортов). Без дополнительной информации, без продуманной системы навигации между всеми проектами и паспортами ориентироваться в них, когда их станет много, было бы. Поэтому было решено добавить к проекту информацию о том, совпал ли он с паспортом, установленным для данного СВТ в момент формирования проекта и имя паспорта, с которым проводилось сравнение. Это позволит даже спустя значительно время просмотреть не просто состояние ПКО в некоторый момент, но знать, в чем именно это состояние отличалось от эталонного, даже если на момент просмотра для СВТ утвержден уже другой паспорт. Такой подход позволяет легко выделять наиболее важные – то есть не совпавшие с паспортом – проекты и при необходимости анализировать именно их.

Также в рамках этой доработки был добавлен еще один механизм, позволяющий сильнее акцентировать внимание пользователя «Паспорта ПО» на проектах, отличных от паспорта СВТ. Любой отличающийся от паспорта находится в статусе «не просмотрен», для перемещения его в архив или превращения в паспорт пользователь должен открыть проект и ознакомиться с его содержимым, подтвердив это действие нажатие кнопки «Просмотрено». Проекты в статусе «не просмотрен» будут постоянно отображаться в интерфейсе как требующие просмотра. Данный механизм обязательного просмотра позволит снизить число инцидентов, при которых один проект не совпал с паспортом, следующий после проекта – совпал, а пользователь «Паспорт ПО», отвечающий за контроль состояния программной среды ПКО, не обратил на это внимание и не произвел необходимых в такой ситуации действий. Но пока данный механизм будет сделан опциональным: его сможет включать/выключать администратор программного модуля, обладающий правом на эту настройку.

Необходимо учесть одно немаловажное последствие такого изменения системы: хранение всех проектов в базе приведет к ее очень быстрому росту, ведь новые проекты создаются гораздо чаще новых паспортов, зачастую ежедневно. На данный момент для оптимизации размеров базы самая объемная часть паспорта – информация о файлах – хранится в базе не в виде строк таблицы, а в серилизованном виде – в байтах. Более того, серилизованные данные еще и дополнительно сжаты архиватором, чтобы занимать еще меньше места. Это позволяет значительно экономить место и экономить время на обращение к базе – вместо тысяч строк таблицы, хранящих данные о файлах, используется одна ячейка для хранения сериализованных упакованных данных. В дальнейшем для экономии места предложено применить аналогичный подход и ко второму по объему элементу паспорта – к информации о продуктах, что, с учетом большого числа проектов, даст значительный выигрыш по памяти.

В такой схеме автоматически удалятся проекты больше не будут, поэтому необходимо добавить ручное удаление проектов. Исходя из опыта общения с пользователями про-

граммного модуля, мы предполагаем, что для проектов будет задан некоторый срок хранения. По истечению, которого проекты и паспорта, сформированные в определенный период времени, будут удалены как устаревшие. в связи с этим было решено сделать механизм, позволяющий удалять сразу большое число проектов или паспортов, указав диапазон дат создания проектов, которые требуется удалить. Так же планируется проработать опцию автоматического удаления проектов, созданных определенное время назад. Заметим, что не просмотренные проекты удаляться не будут никаким способом.

3. Возможность контроля рабочих станций, работающих под управлением ОС семейства Linux. В связи с тенденцией импортозамещения на все большее число рабочих станций в различных организациях устанавливаются операционные системы семейства Linux [4], в связи с этим стал актуальным вопрос контроля ПКО, на которых установлен Linux.

Так как «Паспорт ПО» написан на языке C#, то перенос и запуск клиентского компонента на ОС семестра Linux не вызвал сложностей – потребовались незначительные изменения исходного кода успешного запуска Клиента и осуществления взаимодействия с сервером. Интересной инженерной задачей стало обновление алгоритмов работы Клиента с файловой системой ПКО (опрос исполняемых файлов) и получения списка установленного программного обеспечения.

При работе с файлами основное изменение алгоритма потребовалось ввиду различной логики работы с расширениями файлов с ОС Windows и Linux. В Windows расширения файлов являются неотъемлемой частью имени, используются везде и однозначно характеризуют файл. В Linux расширения файлов необязательны: многие важные файлы, в том числе и бинарные файлы, являющиеся важной характеризующий частью системы, могут вообще не иметь расширений. Сейчас, при работе с ПКО под управлением ОС Windows в шаблоне управляющий персонал «Паспорт ПО» может указать определенные типы файлов, отфильтровав тем самым список опрашиваемых объектов. Это позволяет гибко исключить из опроса те файлы, которые не являются частью ПО или не описывают его конфигурацию.

При работе с ПКО под управлением Linux такой способ не подойдет, нужен другой подход. Включать все файлы в шаблон поименно было бы невероятно трудоемко и сделало бы невозможным использование «Паспорта ПО» в реальных условиях: время опроса ПКО и требуемые на его проведения ресурсы повлекли бы за собой затруднение работы пользователей с контролируемым ПКО.

В итоге было решено ввести понятие исполняемых файлов как совокупности файлов определенных MIME-типов, и позволить пользователям ставить на контроль именно исполняемые файлы.

Был выбран следующий список MIME-типов: application/x-elf; application/x-sharedlib; application/x-dosexec; application/x-object; application/x-executable; application/x-coredump; application/x-perl; application/x-python-code; application/x-php; text/x-shellscript; text/x-python; text/x-perl; text/x-java; text/x-php.

Данные об установленном в системе ПО легко получаются от пакетного менеджера, используемого в текущем клиентском дистрибутиве, наиболее распространенные системы управления пакетами – RPM и dpkg, на данный момент поддержано обращение к этим системам.

4. Возможность контроля аппаратных средств рабочей станции

Несмотря на название продукта – «Паспорт ПО», подразумевающее под собой контроль состояний именно программного обеспечения подконтрольных станций, нельзя забывать, что основная задача, которую решает программный модуль – это контроль целостности конфигураций рабочих мест. Очевидно, что конфигурация рабочего места включает в себя не только программную часть, но и аппаратную, поэтому было решено добавить возможность контроля аппаратной составляющей ПКО.

Список контролируемого оборудования следующий:

1. Processor;
2. BIOS;
3. DiskDevice;
4. Ram;

5. CDROM;
6. USBController;
7. PCI;
8. NetworkAdapter;
9. Motherdoard.

Для каждого элемента определяются следующие данные:

1. Type (тип оборудования, один из вышеперечисленных);
2. Caption;
3. Name;
4. Manufacturer;
5. SerialNumber;
6. Status;
7. ExpDescription (для каждого типа – свой);
8. DeviceName;
9. DeviceId.

В Windows эти данные можно получить из системы через системные вызовы и описание драйверов, в Linux было решено получить это с использованием утилиты Linux Hardware Lister (lshw) – утилиты с открытым исходным кодом, позволяющей собрать данные об аппаратных компонентах текущей рабочей станции [5].

Вывод. Активная обратная связь от пользователей «Паспорта ПО» показывает, что функциональность контроля конфигурации рабочих мест востребована на местах по существу, а не только ради формального удовлетворения требованиям тех или иных регламентов. Не секрет, что это лучший стимул для разработчика, а значит, теоретические исследования и практические разработки в этом направлении будут иметь развитие, и их результатам будут посвящены доклады и на будущих конференциях.

Список литературы

1. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

2. Мозолина, Н. В. Реализация концепции управления конфигурациями при помощи программного модуля «Паспорт ПО» / Н. В. Мозолина // Вопросы защиты информации. – 2020. – № 3. – С. 11–15.

3. Мозолина, Н. В. Дубликатом бесценного груза: «Паспорт ПО» / Н. В. Мозолина // Information Security/Информационная безопасность. – 2020. – № 5. – С. 46–47.

4. Госорганы России массово меняют Windows на Astra Linux [Электронный ресурс]. – Режим доступа : https://www.cnews.ru/news/top/2020-11-12_gosorgany_rossii_massovo. – Дата доступа : 06.05.2021.

5. Hardware Lister (lshw) [Электроный ресурс]. – Режим доступа : https://ezix.org/project/wiki/HardwareLiSter. – Дата доступа : 06.05.2021.

УДК 621.396; 534.41

ПОВЫШЕНИЕ ТОЧНОСТИ ОЦЕНКИ ПАРАМЕТРОВ СЛОЖНЫХ СИГНАЛОВ ПРИ ВЫСОКОЙ ЧАСТОТЕ ДИСКРЕТИЗАЦИИ

И.Б. БУРАЧЕНОК, В.К. ЖЕЛЕЗНЯК, С.В. ЛАВРОВ
Учреждение образования «Полоцкий государственный университет», Новополоцк, 211446, Республика Беларусь

А.Г. ФИЛИППОВИЧ, М.М. БАРАНОВСКИЙ
Оперативно-аналитический центр при Президенте Республики Беларусь, г. Минск, 220030, Республика Беларусь

Введение. Информационные речевые сигналы (РС), формируемые первичными преобразователями из передаваемого сообщения, представлены множеством параметров и различными формами [1]. Такие сигналы подвергаются помеховым возмущениям в каналах утечки информации (КУИ) и не могут воспроизводиться идеально. Точность вычислений при этом зависит от того, насколько точно будут восстановлены РС при аналогово-цифровом (АЦП) и цифро-аналоговом (ЦАП) преобразованиях, а погрешность восстановления исходного РС зависит от: вида исходной функции; процесса квантования, связанного с округлением значений непрерывного сигнала; интервала квантования и алгоритма восстановления. Дискретизация сигналов приводит к определенной потере информации о поведении сигналов в промежутках между отсчетами за счет возникновения дополнительных спектральных составляющих, поэтому возникает необходимость в дополнительном исследовании тонкой структуры сигнала, представленного периодической последовательностью импульсов дискретизации.

Цель работы: анализ тонкой структуры спектральных составляющих, обусловленных дискретным преобразованием аналоговых речевых сигналов в каналах утечки информации.

Основной задачей является исследование аналогово-цифрового преобразования разложением произвольной функции на элементарные δ-импульсы и анализ информации о совокупном значении численных величин параметров шума квантования при дискретно-квантованном представлении РС в КУИ.

Итак, дискретный сигнал по своим значениям в процессе анализа может быть разложен только по системам дискретных базисных функций, у которых отсчеты времени совпадают с отсчетами сигнала, т. е. по сути он является непрерывной функцией, но определенной только по дискретным значениям аргумента [2]. По множеству своих значений он является конечным и описывается дискретной последовательностью отсчетов $y\left(n\Delta t\right)$, где $y_1 \le y \le y_2$, Δt – интервал между отсчетами, т. е. дискретный сигнал представляет собой последовательность отсчетов, значения которых в точности равны значениям исходного сигнала по координатам $n\Delta t$. Частота дискретизации при этом $f = 1/\Delta t,\ \Delta t$ – является величиной, обратной шагу дискретизации.

Если же рассматривать цифровой сигнал, то он квантован по своим значениям и дискретен по аргументу. Такой сигнал описывается квантованной решетчатой функцией [3] $y_n = Q_k\left[\left(n\Delta t\right)\right]\left(n\Delta t\right)$, где Q_k – функция квантования с числом уровней квантования k, при этом интервалы квантования могут быть как с равномерным распределением, так и с неравномерным. Ранее в работе [4] приводится обоснование выбранного равномерного шага квантования.

По существу, цифровой сигнал по своим отсчетам является формализованной разновидностью дискретного сигнала. Процесс преобразования бесконечных по значениям аналоговых отсчетов в конечное число цифровых значений называется квантованием по уровню. Возникающие при квантовании ошибки округления до определенного количества цифр отсчетов и есть шумы или ошибки квантования, которые зависят в том числе и от частоты дискретизации, порождающей дополнительные спектральные составляющие.

В системах цифровой обработки данных и в ЭВМ сигнал всегда представлен с точностью до определенного количества разрядов, а, следовательно, всегда является цифровым [2]. С учетом этих факторов при описании цифровых сигналов функция квантования обычно опускается (подразумевается равномерной по умолчанию), а для описания сигналов используются правила описания дискретных сигналов. Причем при дискретизации сетка отсчетов по аргументу может быть произвольной или задаваться по определенному закону.

Сегодня широко применяются методы равномерной дискретизации, так как при их использовании алгоритмы дискретизации и восстановления сигналов и соответствующая аппаратура просты в реализации, поэтому далее рассмотрим равномерную дискретизацию по времени (с постоянным шагом по аргументу), при $s(t) \Rightarrow s(n\Delta t)$, где значения $s(n\Delta t)$ представляют собой отсчеты функции $s(t)$ в моменты времени $t = n\Delta t,\ n = 0,1,2.....N$. Примером дискретного сигнала с квантованием по времени является модулированная по амплитуде последовательность идеальных импульсов равной длительности Δ, представленная в виде ступенчатой функции $x_\Delta(t)$, имеющей в каждом интервале постоянное значение, равное значению функции $x(t)$ в середине этого интервала, как показано на рисунке 1.

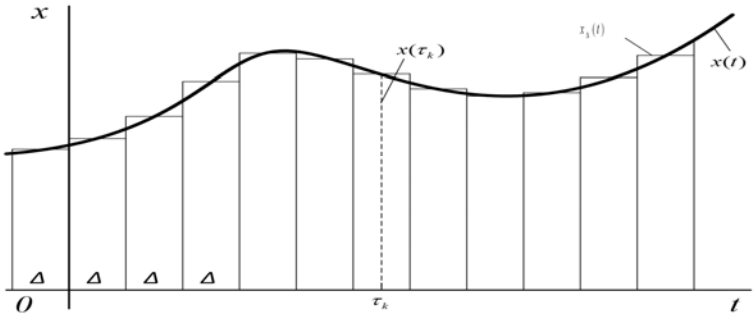


Рис. 1. Ступенчатая функция

Обозначим середину k-того интервала через $\tau_k (k = 0, \pm1, \pm2, ...)$. Значение функции $x(t)$ в точке τ_k, равно $x(\tau_k)$. Построим прямоугольный импульс длительности Δ, имеющий высоту $x(\tau_k)$ (рис. 2).

Если единичный импульс конечной длительности Δ (высота этого импульса равна $1/\Delta$) представить выражением [5]

$$\delta_\Delta(t) = \begin{cases} \dfrac{1}{\Delta} & \text{при } |t| < \dfrac{\Delta}{2}, \\ 0 & \text{при } |t| > \dfrac{\Delta}{2}. \end{cases} \qquad (1)$$

то отдельный прямоугольный импульс, действующий в промежутке времени $\left(\tau_k - \dfrac{\Delta}{2}, \tau_k + \dfrac{\Delta}{2}\right)$, можно представить в виде функции $\delta_\Delta(t - \tau_k)$.

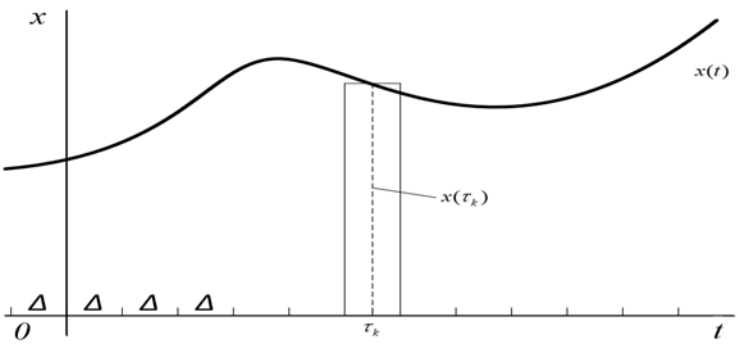


Рис. 2. Прямоугольный импульс длительностью Δ, построенный на k-том интервале ступенчатой функции

Чтобы получить импульс высотой $x(\tau_k)$, необходимо функцию $\delta_\Delta(t-\tau_k)$ умножить на $x(\tau_k)$ и разделить на $\frac{1}{\Delta}$, в результате получим $\delta_\Delta(t-\tau_k)x(\tau_k)\Delta$. Сумма таких импульсов по всем интервалам, на которые разбили ось t, представляет ступенчатую функцию, имеющую в каждом интервале постоянное значение, равное значению функции $x(t)$ в середине этого интервала

$$x_\Delta(t)=\sum_{k=-\infty}^{\infty}\delta_\Delta(t-\tau_k)x(\tau_k)\Delta. \qquad (2)$$

Из полученного выражения (2) однозначно следует, что на точность передачи аналогового сигнала значительно влияет длительность импульса дискретизации.

Подробнее остановимся на рассмотрении идеального единичного δ-импульса, представленного сигналом в виде так называемой δ-функции [6]. Импульсная δ-функция впервые введена в науку знаменитым английским физиком Дираком. Импульсной δ-функцией называется функция, равная нулю всюду, кроме начала координат, принимающая бесконечное значение в начале координат $\delta(t)=0$ при $t\neq 0$, $\delta(0)=\infty$, и при том так, что интеграл от нее по любому интервалу, содержащему начало координат, равен единице $\int_{-\varepsilon}^{\varepsilon}\delta(t)dt=1$ при любом $\varepsilon>0$.

Данная функция обладает следующими свойствами: это функция времени, которая имеет бесконечно большое значение в течение определенного бесконечно малого промежутка и равна нулю вне этого промежутка времени. Интеграл от такой функции конечен и равен мгновенному изменению скорости тела. Функцию, обладающую такими свойствами, можно получить, например, как предел положительного прямоугольного импульса, имеющего единичную площадь, когда длительность этого импульса стремиться к нулю. График такой функции можно представить, как показано на рисунке 3.

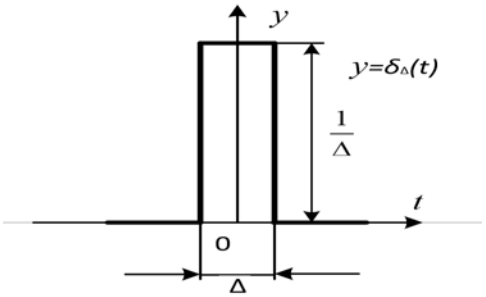


Рис. 3. Положительный прямоугольный импульс единичной площади

Чем уже полоска между левой и правой частью, тем выше она должна быть для того, чтобы ее площадь (т. е. интеграл) сохраняла свое заданное значение, равное 1. При сужении полоски приближаемся к выполнению условия $\delta(t) = 0$ при $t\neq 0$.

Еще удобнее определить δ-функцию как предел при $h\to\infty$ функции

$$\delta_h(t)=\frac{h}{\sqrt{\pi}}e^{-h^2t^2}. \qquad (3)$$

Очевидно, что при любом $t\neq 0$ функция $\delta_h(t)$ стремиться к нулю при $h\to\infty$. При $t=0$ эта функция неограниченно возрастает при $h\to\infty$. Наконец, при любом $\varepsilon>0$ имеем выражение

$$\int_{-\varepsilon}^{\varepsilon}\delta_h(t)dt=\frac{h}{\sqrt{\pi}}\int_{-\varepsilon}^{\varepsilon}e^{-h^2t^2}dt=\frac{1}{\sqrt{\pi}}\int_{-h\varepsilon}^{h\varepsilon}e^{-u^2}du\ . \qquad (4)$$

При $h\to\infty$ – это выражение стремиться к единице. Важно также, чтобы δ-функция была четной.

Преобразование Фурье единичного импульса имеет вид $F[\delta(t)]=\int_{-\infty}^{\infty}\delta(t)e^{-i\omega t}dt$ и равно единице: $F[\delta(t)]=1$ [5], как показано на рисунке 4.

Рис. 4. Преобразование Фурье, включающее единичный импульс

Это означает, что единичный импульс имеет равномерную спектральную плотность во всей бесконечной области частот, т. е. единичный импульс содержит составляющие всех возможных частот ω с одинаковыми относительными амплитудами. Преобразование Фурье δ-функции показало, что ее площадь не убывает с ростом частоты и остается неизменной, т. е. равной единице.

Следующим этапом рассмотрим периодическую последовательность единичных импульсов. Если задать время повторения импульсов $T_{сек}$, то такую последовательность можно представить следующим выражением [7]

$$\delta_T(t)=\delta(t)+\delta(t-T)+\delta(t-2T)+...+\delta(t-nT)+...$$
$$+\delta(t+T)+\delta(t+2T)+...+\delta(t+nT)+...=\sum_{n=-\infty}^{\infty}\delta(t-nT)\ . \qquad (5)$$

Осуществим преобразование Фурье от периодической последовательности единичных импульсов и получим $\delta_T(t)=\sum_{n=-\infty}^{\infty}F_n e^{in\omega_0 t}$, где $F_n=\int_{-T/2}^{T/2}\delta_T(t)e^{-in\omega_0 t}dt$.

На интервале $\left(-\frac{T}{2},\frac{T}{2}\right)$ функция $\delta_T(t)$ есть единичный импульс $\delta(t)$. Следовательно,

$$F_n=\frac{1}{T}\int_{-T/2}^{T/2}\delta(t)e^{-in\omega_0 t}dt\ . \qquad (6)$$

В силу фильтрующего свойства единичного импульса [5] полученное соотношение оказывается равным $F_n=\frac{1}{T}$, т. е. постоянной величине, это означает, что периодическая последовательность единичных импульсов с периодом T содержит составляющие с частотами $\omega=0,\ \pm\omega_0,\ \pm2\omega_0,\ ...,\ \pm n\omega_0,\ ...$ и т. д. $\left(\omega_0=\frac{2\pi}{T}\right)$ одинаковой амплитудой $\delta_T(t)=\frac{1}{T}\sum_{n=-\infty}^{\infty}e^{in\omega_0 t}$.

Чтобы найти преобразование Фурье от $\delta_T(t)$, воспользуемся функцией спектральной плотности или преобразованием Фурье периодической функции из единичных импульсов, расположенных на частотах гармоник сигнала, с интенсивностями в 2π раз больше соответствующих коэффициентов экспоненциального ряда Фурье $F[f(t)]=2\pi\sum_{n=-\infty}^{\infty}F_n\delta(\omega-n\omega_0)$. Так как в нашем случае $F_n=\frac{1}{T}$, то имеем

$$F\left[\delta_T(t)\right]=2\pi\sum_{n=-\infty}^{\infty}\frac{1}{T}\delta(\omega-n\omega_0)=\frac{2\pi}{T}\sum_{n=-\infty}^{\infty}\delta(\omega-n\omega_0)=\omega_0\sum_{n=-\infty}^{\infty}\delta(\omega-n\omega_0)=\omega_0\delta_{\omega_0}(\omega). \quad (7)$$

Полученное соотношение (7) устанавливает, что преобразование Фурье периодической последовательности единичных импульсов с периодом T есть последовательность единичных импульсов с одинаковыми амплитудами, разделенными интервалами ω_0,рад $\left(\omega_0=\frac{2\pi}{2}\right)$.

Полученные периодические последовательности единичных импульсов с периодами и их соответствующие преобразования Фурье показаны на рисунке 5.

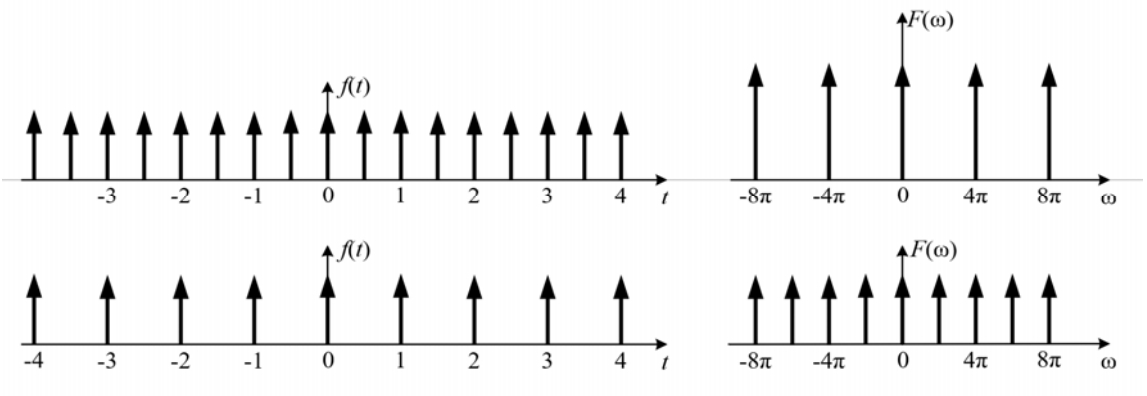


Рис. 5. Периодические последовательности единичных функций и их преобразование Фурье

Очевидно, что при увеличении периода частотный спектр становится плотнее, увеличивается частота дискретизации и снижаются ошибки квантования.

Таким образом, анализ тонкой структуры спектральных составляющих, обусловленных дискретным преобразованием аналоговых речевых сигналов показывает возникновение дополнительных КУИ и пути повышения точности.

Погрешность дискретизации можно оценить следующим образом

$$\varepsilon(t)=x(t)-V(t), \quad (8)$$

где $x(t)$ – истинное значение сигнала, $V(t)$ – полученное после восстановления.

Чаще других отклонений воспроизводимой функции $V(t)$ от сигнала $x(t)$ на интервале дискретизации оценивается следующими критериями [8].

1. Критерий наибольшего отклонения

$$\varepsilon_m=\max_{t\in\Delta T_i}\left|\varepsilon(t)\right|=\max_{t\in\Delta T_i}\left|x(t)-V(t)\right|, \quad (9)$$

где $\varepsilon(t)$ – текущая погрешность, определяемая выражением (8).

2. Среднеквадратический критерий, определяемый следующим выражением:

$$\overline{\varepsilon}^2=\sqrt{\frac{1}{\Delta T_i}\int_{\Delta T_i}\varepsilon^2(t)dt}=\sqrt{\frac{1}{\Delta T_i}\int_{\Delta T_i}\left|x(t)-V(t)\right|^2dt}, \quad (10)$$

где $\varepsilon(t)$ – текущая погрешность, определяемая выражением (8).

3. Интегральный критерий как мера отклонения $x(t)$ от $V(t)$, определяемый выражением

$$\overline{\varepsilon}=\int_{\Delta T_i}\varepsilon(t)dt. \quad (11)$$

4. Вероятностный критерий, определяемый соотношением

$$p=\{\varepsilon(t)<\varepsilon_0\}=p_0, \tag{12}$$

где ε_0 – допустимое значение погрешности; p_0 – допустимая вероятность того, что погрешность не превысит значения ε_0.

В приведенных определениях критериев отклонений не приводится весовая функция. Введение весовой функции позволяет заменить истинную погрешность взвешенной. Для множества реализаций критерий наибольшего отклонения может быть записан в следующем виде: $E_m=\sup\{\varepsilon_m\}$, где верхняя грань отыскивается по всем реализациям $x(t)$ и $V(t)$.

Заключение. В работе показано, что при преобразовании аналогового сигнала в цифровой и обратно операции АЦП и ЦАП не являются взаимно обратными с абсолютной точностью. Ошибки, обусловленные дискретным преобразованием аналоговых РС, имеют собственное спектральное распределение, которое зависит от параметров АЦП, частоты и формы исходного сигнала. Исследования тонкой структуры спектральных составляющих, обусловленных дискретным преобразованием аналоговых РС, позволяет обнаруживать гармоники шума квантования в КУИ и судить о характеристиках передаваемого РС. Также показано, что ограничение ошибок квантования требует повышения частоты дискретизации. При выборе равномерной частоты дискретизации большую роль играет выбор частоты отсчетов (шаг дискретизации). В нашем случае при оценке КУИ в диапазоне РС от 100 до 10кГц для снижения погрешности квантования принято решение использовать частоту дискретизации 192 кГц (интервал дискретизации 5,2 мкс), что значительно повышает точность оценки параметров сложных сигналов.

Список литературы

1. Бураченок, И. Б. Обнаружение первичных признаков речевого сигнала / И. Б. Бураченок, В. К. Железняк // Вестник Полоцкого государственного университета. Серия С. Фундаментальные науки. – 2020. – № 12. – С. 2–12.

2. Давыдов А. В. Сигналы и линейные системы : тематические лекции. – Екатеринбург : УГГУ ; ИГиГ ; Фонд электр. документов, 2005.

3. Бессонов, Л. А. Линейные электрические цепи : учеб. пособие для электротехнич. и радиотехнич. специальностей вузов / Л. А. Бессонов. – Изд. 2-е, перераб. и доп.– М. : Высш. шк., 1974. – 320 с.

4. Железняк, В. К. Некоторые проблемы оценки защищенности шума квантования / В. К. Железняк [и др.] // ВГАС «Проблемы инфокоммуникаций» – 2020. – № 2 (12). – С. 60–65.

5. Основы автоматического управления / под ред. В. С. Пугачева. – М. : Наука, 1974. – 720 с.

6. Солодов А. В. Теория информации и ее применение к задачам автоматического управления и контроля / А. В. Солодов. – М. : Наука, 1967. – 432 с.

7. Лахтин, Б. П. Системы передачи информации. / Б. П. Лахтин / пер. С англ. ; под общ. ред. Б. И. Кувшинова. – М. : Связь, 1971. – 324 с.

8. Темников, Ф. Е. Теоретические основы информационной техники : учеб. пособие для вузов / Ф. Е. Темников, В. А. Афомин, В. И. Дмитриев. – 2-е изд., перераб. и доп. – М. : Энергия, 1979. – 512 с.

УДК 004.056

ПРИМЕНЕНИЕ ИЗВЕСТНЫХ АЛГОРИТМОВ ТЕОРИИ ГРАФОВ ДЛЯ ТЕСТИРОВАНИЯ ФУНКЦИЙ БЕЗОПАСНОСТИ ПРОГРАММНО-АППАРАТНЫХ СЗИ

Т.М. КАННЕР
Закрытое акционерное общество «ОКБ САПР»,
г. Москва, Российская Федерация

В настоящее время все чаще подходы к тестированию программных или программно-аппаратных комплексов, в том числе и средств защиты информации (СЗИ), предполагают построение математических моделей с использованием некоторого математического аппарата, чаще всего теории автоматов [1–4]. При этом поведение СЗИ моделируется с помощью выполнения переходов автомата и получения выходных значений. По аналогии с этими работами в одной из предыдущих работ автора [5] разработана описательная и на ее основе формальная модель произвольного программно-аппаратного СЗИ, для которой сформированы необходимые и достаточные условия принципиальной возможности проведения тестирования. В следующей работе автора [6] на основании математической модели программно-аппаратного СЗИ предложено его представление в виде автомата.

Подходы, основанные на использовании теории автоматов, в том числе и описанный автором в [6], можно использовать для обеспечения полноты тестирования программно-аппаратных средств защиты информации. Однако вопрос оптимальности тестирования при применении этих подходов остается открытым. Для обеспечения не только полноты, но и оптимальности в [6] автором сформулирована задача тестирования программно-аппаратного СЗИ, на основании которой предложен подход к проверке ее выполнимости с использованием положений теории графов.

В данной статье автором предлагается основанный на предложенном в [6] подходе алгоритм тестирования функций безопасности программно-аппаратных СЗИ, использующий известные алгоритмы теории графов, и позволяющий провести тестирование функций безопасности таких СЗИ, а также обеспечить его полноту и оптимальность.

Введем по аналогии с [6] граф, соответствующий программно-аппаратному СЗИ, представленному в виде формальной модели в [5]:

$G_m = (V, E)$ – ориентированный граф без петель и кратных дуг (простой орграф), где V – множество вершин графа, соответствующих состояниям программной или аппаратной компоненты СЗИ, а $E \subseteq V \times V$ – множество ориентированных ребер (дуг) графа – переходов СЗИ из одного состояния в другое при выполнении нецелевых функций или функций безопасности.

Задача тестирования заключается в обходе из некоторой начальной вершины $v_0 \in V$ всех дуг графа, входящих в вершины, в которых могут выполняться какие-либо функции безопасности СЗИ – $V_{фб} \subseteq V$. При этом обеспечение полноты и оптимальности тестирования основано на поиске пути, проходящего через все дуги хотя бы по одному разу за минимальное количество переходов. Таким образом, в соответствии с [6–9] задача тестирования сводится к задаче китайского почтальона (англ. Chinese postman problem), также известной как задача инспекции дорог (англ. Route Inspection Problem), либо, как частный случай – к задаче поиска Эйлерова пути (англ. Eulerian path / Eulerian trail).

На основе введенного представления программно-аппаратного СЗИ в виде графа предложен алгоритм решения задачи тестирования функций безопасности программно-аппаратного СЗИ, который заключается в выполнении следующих шагов:

1. Построить из изначального графа программно-аппаратного СЗИ G_m соответствующий граф G'_m с помощью удаления неиспользуемых при решении задачи тестирования не-

которых вершин и дуг, используя приведенные в [6] правила для сохранения связности оставшихся вершин.

2. Если в G'_m есть изолированные вершины (не удаленные при построении графа G_m) – задача тестирования не может быть решена, так как невозможно будет выполнить условие полноты тестирования из [6].

3. Проверить, что в G'_m любая вершина $v \in V$ либо принадлежит орцепи, либо лежит в компоненте сильной связности, то есть имеет вид как на рисунке 1.

4. Это можно сделать с использованием алгоритма Косараджу-Шарира за два обхода графа в глубину [7, 10, 11]: найти все компоненты связности и проверить связанность начальной вершины v_0 со всеми остальными вершинами. В противном случае задача тестирования не может быть решена, так как также невозможно будет выполнить условие полноты из [6].

5. Для всех вершин графа G'_m необходимо вычислить разницу полустепеней выхода от полустепеней входа. Если в графе есть только сбалансированные вершины (разница равна *«0»)*, то в графе существует Эйлеров цикл. Если в графе есть только две несбалансированные вершины с разницей *«*1*»* и «-1*»*, а остальные вершины сбалансированные, то в графе существует Эйлеров путь. В этих случаях необходимо продолжить алгоритм с пункта 9.

6. В противном случае рассмотреть отдельно несбалансированные вершины с целью нахождения путей, которые необходимо пройти повторно с сохранением требования по минимизации обхода дуг из условия оптимальности тестирования в [6]. Несбалансированные вершины можно представить в виде биграфа.

7. С помощью алгоритма поиска кратчайших путей для всех вершин в полученном биграфе – алгоритма Флойда-Уоршелла [7, 10], вычислить длину кратчайших путей от вершин с отрицательной разницей полустепеней выхода и входа к вершинам с положительной разницей.

8. Выбрать с использованием Венгерского алгоритма, алгоритма Куна-Манкреса или алгоритма Форда-Фалкерсона [7, 10] из всех сочетаний возможных кратчайших путей те пути, при повторном использовании которых все вершины станут сбалансированными, но при этом суммарная длина этих путей будет минимальна. При добавлении пути от вершины с отрицательной разницей полустепеней выхода и захода к вершине с положительной разницей, разница в обеих вершинах изменится ровно на «1» (для первой увеличится на *«*1*»*, для второй уменьшится на *«*1*»*). При этом для всех остальных вершин разница не изменится, так как могут добавиться только входящая и исходящая дуга (суммарная разница останется *«*0*»*).

9. Добавить дуги для выбранных на предыдущем шаге дополнительных путей в граф G'_m. Так как теперь все вершины сбалансированы, то будет существовать Эйлеров цикл.

10. С помощью алгоритма на основе циклов, также известного как алгоритм Хиерхольцера [9], построить Эйлеров цикл в полученном графе. Посещение достроенных на предыдущем шаге дуг эквивалентно повторному посещению соответствующих дуг графа G'_m. Некоторые итерации Эйлерова цикла можно менять местами, так как оптимальное решение может быть не единственным.

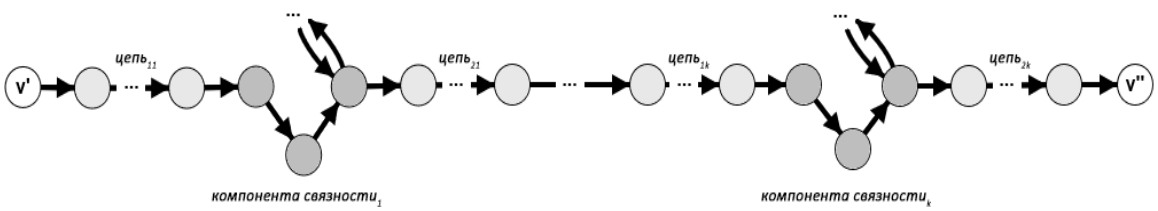


Рис.1. Общий вид графа для решения задачи тестирования – отдельные вершины, цепи или компоненты связности могут отсутствовать, $k \in N_0$

Блок-схема предложенного алгоритма тестирования приведена на рисунке 2.

Из предложенного алгоритма решения задачи тестирования программно-аппаратных СЗИ видно, что его шаги выполняются последовательно, и для них не используется вложен-

ность. Это означает, что сложность представленного алгоритма равна максимальной сложности используемых в нем известных алгоритмов на графах.

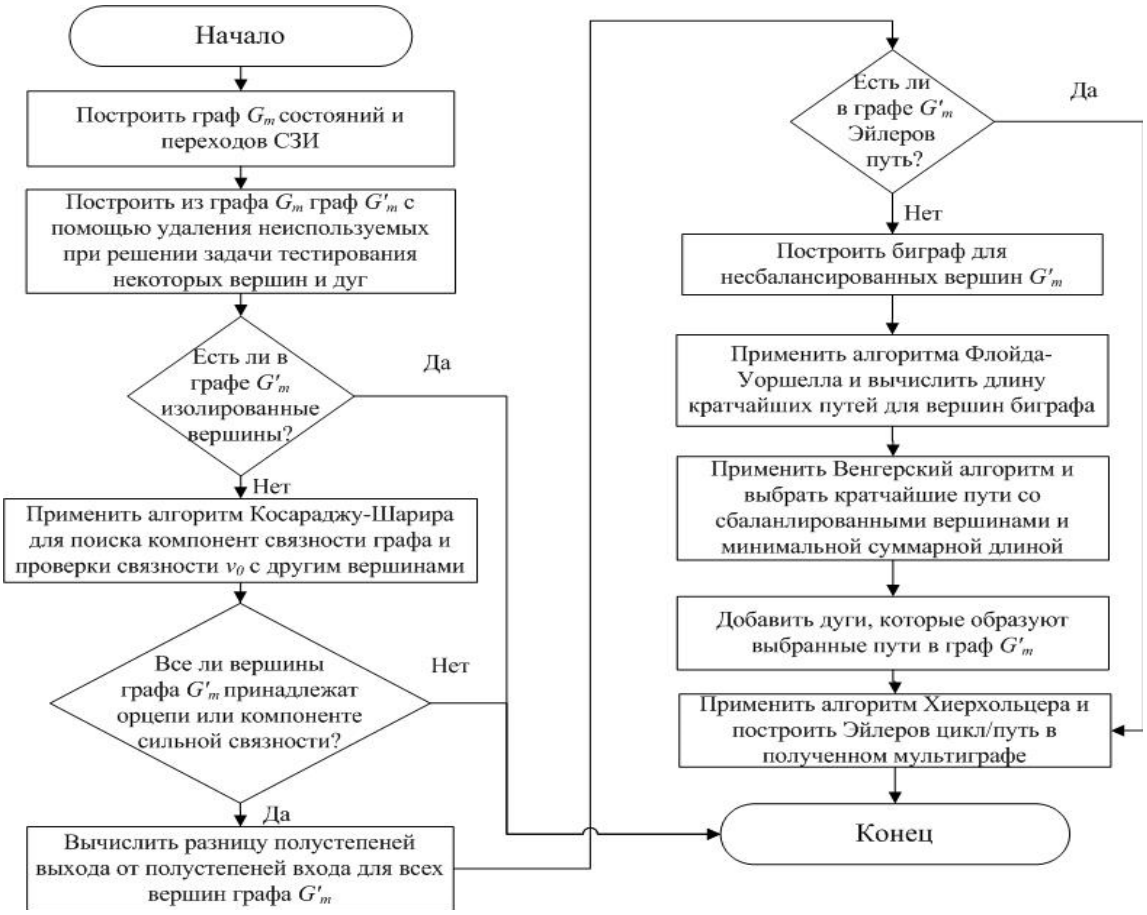


Рис. 1. Блок-схема алгоритма решения задачи тестирования функций безопасности программно-аппаратных СЗИ

Сложности используемых алгоритмов, следующие [6, 7, 9]:

1. Сложность построения графа G'_m для представления графа в виде матрицы смежности $O(|V'|^3)$. За $O(|V'|^3)$ выполняется первая проверка при построении G'_m, за $O(|V'|^2)$ – вторая и третья, а четвертая проверка – за $O(|V'|^3)$. Соответственно общая сложность не будет превосходить сложности первой или четвертой проверки.
2. Алгоритм Косараджу-Шарира – $O(|V'|^2)$ для матрицы смежности;
3. Рассчет полустепеней выхода и входа и их разницы для каждой вершины – $O(|V'|^2)$ для матрицы смежности;
4. Алгоритм Флойда–Уоршелла – $O(|V'|^3)$;
5. Венгерский алгоритм – $O(|V'|^3)$;
6. Алгоритм Хиерхольцера – $O(|E'|)$.

То есть в случае если G'_m содержит Эйлеров путь (цикл) или не содержит – сложность алгоритма будет $O(|V'|^3)$ для представления графа в виде матрицы смежности. То есть задача тестирования программно-аппаратных СЗИ принадлежит классу задач P, а не NP и существует алгоритм, решающий эту задачу за полиномиальное время [9].

Предложенный алгоритм подразумевает обход вершин графа с помощью одной последовательности переходов. В случае если обход графа по приведенному алгоритму невозможно выполнить с помощью одной последовательности переходов, то это означает, что в графе есть несколько несвязанных ветвей. А это значит, что в СЗИ есть ошибка, так как нельзя добиться, чтобы все функции безопасности выполнялись корректно без нарушения работы других функций безопасности. Поэтому в работе не рассматривается вариант с несколькими последовательными обходами графа СЗИ.

Проведена апробация предложенного алгоритма на практике – для решения задачи тестирования двух произвольно выбранных программно-аппаратных СЗИ различных видов: ШИПКА – функции безопасности которого реализованы на базе мобильной аппаратной компоненты и взаимодействуют со средой ОС средства вычислительной техники (СВТ) и СЗИ от несанкционированного доступа «Аккорд-АМДЗ» – функции безопасности которого реализованы на базе стационарной аппаратной компоненты и не взаимодействуют с ОС СВТ, выполняются независимо от ОС в составе СВТ [5]. Для данных СЗИ построены соответствующие графы, применен предложенный алгоритм и показано, что задача тестирования для данных СЗИ может быть решена, так как оба графа для них являются сильно связными. Это значит, что по предложенному алгоритму для них можно построить оптимальный путь, проходящий по всем ребрам, то есть обеспечить полноту и оптимальность тестирования.

Таким образом, в статье предложен алгоритм решения задачи тестирования произвольного программно-аппаратного СЗИ с использованием положений теории графов и известных алгоритмов на графах. В соответствии с данным алгоритмом для некоторых программно-аппаратных средств защиты эту задачу решить невозможно, так как не все вершины графа принадлежат орцепи или компоненте сильной связности, для остальных СЗИ задача имеет решение в худшем случае за полиномиальное время.

Список литературы

1. Beizer, B. Software testing techniques / B. Beizer. – Dreamtech, 2003.
2. Model based testing of reactive systems / M. Broy [et al.]. – LNCS 3472, Springer Berlin Heidelberg, 2005.
3. Кулямин, В. В. Тестирование на основе моделей : курс лекции ВМиК МГУ [Электронный ресурс]. – Режим доступа : http://panda.ispras.ru/~kuliamin/mbt-course.html. – Дата доступа : 07.04.2021.
4. Бурдонов, И. Б. Использование конечных автоматов для тестирования программ / И. Б. Бурдонов // Программирование. – 2000. – № 2. – С. 12–28.
5. Glob, J. Applicability of software testing methods to software and hardware data security tools / J. Glob // Pure Appl. Math. – 2016. – Vol. 12 (1). – P. 167–190.
6. Kanner, T. M. Testing Software and Hardware Data Security Tools Using the Automata Theory and the Graph Theory / A. M. Kanner, T. M. Kanner // Proceedings of Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology. – 2020. – P. 615–618.
7. Седжвик, Р. Фундаментальные алгоритмы на С. Часть 5: Алгоритмы на графах / Р. Седжвик. – 3-е изд. – СПб. : ДиаСофтЮП, 2003. – 496 с.
8. Edmonds, J. Matching Euler tours and the chinese postman / E. L. Johnson, J. Edmonds // Mathematical programming. – 1973. – Vol. 5 (1). – P. 88–124.
9. Скиена, С. С. Алгоритмы. Руководство по разработке / С. С. Скиена ; пер. С англ. – 2-е изд. – СПб. : БХВ-Петербург, 2018.
10. Кормен, Т. Алгоритмы: построение и анализ / Т. Кормен [и др.]. – 3-е изд. – М. : Вильямс, 2013. – 1328 с.
11. Sharir, M. A strong connectivity algorithm and its applications to data flow analysis / M. Sharir // Computers and Mathematics with Applications. 1981. – Vol. 7 (1). – P. 67–72.

УДК 004.056

СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДОЛЖНОСТНЫМИ ЛИЦАМИ О РАЗМЕЩЕНИИ ПЕРСПЕКТИВНЫХ КОМПЛЕКСОВ ОХРАНЫ УЧАСТКОВ ГОСУДАРСТВЕННОЙ ГРАНИЦЫ

Л.Л. УТИН, Е.Л. ОСТРОМУХОВ
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»,
Открытое акционерное общество «Научно-исследовательский институт электронных вычислительных машин», г. Минск, Республика Беларусь

Введение. В настоящее время выбор тех или иных средств инженерно-технической защиты, как правило, осуществляется на основе здравого смысла, имеющегося опыта и интуиции лица, принимающего решение (далее – ЛПР). В лучшем случае для принятия решений приглашаются эксперты в области защиты информации, в худшем – решения принимаются индивидуально. Из-за большого количества альтернативных вариантов по применению существующих средств обнаружения, видеонаблюдения и сигнализации, ограниченных психофизиологических возможностей, присущих природе любого человека, отсутствия специализированных компьютерных программ оптимизации применения выбранных средств, ЛПР затрачивает много времени для построения системы защиты. Такой подход не всегда способствует и оптимальному расходованию финансовых средств, выделенных на обеспечение защиты информации.

Основная часть. В [1] было показано, что повышение спроса на системы инженерно-технической защиты способствовало появлению определенной конкуренции у производителей соответствующего оборудования. В результате в настоящее время известно множество компаний, которые занимаются монтажом технических средств охраны. Однако следует отметить, что поставляемое ими оборудование, как правило, является разработкой иностранных компаний. Не смотря на кажущуюся низкую стоимость предлагаемого оборудования, допуск таких компаний для монтажа систем охраны государственной границы может иметь далеко идущие негативные последствия для государства.

В [2] были рассмотрены основные направления совершенствования систем охраны протяженных периметров. Было показано, что одним из оригинальных решений является применение комплекса ВМ8018, разработанного в ОАО «Научно-исследовательский институт электронных вычислительных машин». Данный комплекс предназначен для автоматизации процесса охраны протяженных периметров объектов различного назначения, в том числе участков государственной границы, периметров и помещений застав, протяженных периметров промышленных и военных объектов, а также управления исполнительными устройствами (электроприводами ворот и калиток, освещением и т. п.), ведения видеонаблюдения, защищенного документирования событий [3].

Для повышения обоснованности принимаемых решений по размещению элементов комплекса вдоль участков охраняемого периметра следует разработать и использовать соответствующие средства принятия решений. Данные средства должны обеспечивать возможность:

– работы лица, принимающего решение, напрямую с требуемой ему информацией без посредников;

– моделирования конструктивных особенностей охраняемого периметра, подключения различных типов датчиков, а также погодных условий;

– формирования множества альтернативных вариантов размещения элементов комплекса и отображение их на карте местности;

– хранения в базах данных сведений о технических характеристиках существующих средств обнаружения и особенностях их размещения на местности.

Кроме этого, разрабатываемые средства поддержки принятия решений должны быть гибкими и легко адаптируемыми к конструктивным особенностям охраняемого периметра, легко модифицироваться в соответствии с изменяющимися характеристиками комплекса.

Основываясь на теории принятия решений, было предложено в основу разрабатываемой программы положить пять основных компонентов:

1. База данных, предназначенная для хранения исходной информации об технических характеристиках средств обнаружения, параметрах соединительных линий и возможностях элементов комплекса, а также с данными о командах голосового оповещения при срабатывании средств обнаружения и обрыве соединительных линий. Кроме того, в этой базе хранится ранее сформированная конфигурация размещения элементов комплекса, средств обнаружения и исполнительных устройств, необходимых для нахождения допустимых и оптимальных альтернатив;

2. Модуль управления предназначен для формирования управляющих команд на выдачу в блок моделирования требуемых исходных данных, команд запроса из модуля аналитики об альтернативных решениях и команд вывода информации из модуля отчетности;

3. Блок моделирования предназначен для имитации размещения элементов комплекса вдоль охраняемого периметра, а также проведения требуемых математических расчетов;

4. Модуль аналитики обеспечивает анализ допустимых вариантов решения поставленной задачи и определения из них рациональных (квазиоптимальных по заданным показателям и критериям);

5. В модуле отчетности осуществляется хранение результатов исследований.

Самым важным компонентом программного комплекса является блок аналитики, так как остальные компоненты являются обеспечивающими и вспомогательными. Основу модуля аналитики составляет математическое обеспечение для решения оптимизационной задачи о минимизации требуемого количества блоков линейных комплекса ВМ8018 в зависимости от подключаемой нагрузки и протяженности охраняемого участка.

Математическая модель оптимизации была реализована в виде алгоритма и далее внедрена в компьютерную программу. Данная компьютерная программа поддержки принятия решений была апробирована в ходе опытной эксплуатации комплекса ВМ8018.

Заключение. Развитие информационных технологий позволило создавать компьютерные программы, которые позволяют должностным лицам, отвечающим за планирование и реализацию внедрения мер инженерно-технической защиты, в короткие сроки принимать обоснованные решения на выбор и размещение перспективных средств охраны протяженных периметров с учетом подключения разнообразных средств обнаружения. В докладе рассмотрено одно из возможных решений частной задачи по оптимизации размещения средств перспективного комплекса ВМ8018.

Список литературы

1. Утин, Л. Л. Перспективные направления совершенствования систем охраны протяженных периметров : мат-лы докл. науч.-практ. конф. «Комплексная защита информации», Москва, 15-17 сентября 2020 г./ Л. Л. Утин, Е. Л.Остромухов, А. М. Солонович. – М., 2020. – С. 218–220.

2. Утин, Л. Л. Обзор возможностей отечественного комплекса нового поколения для охраны протяженных периметров тезисы : мат-лы респ. науч.-практич. конф. «Актуальные проблемы обеспечения общественной безопасности в Республике Беларусь : теория и практика», Минск, 21 мая 2020 г. / Л. Л. Утин, А. В. Павловский, А. П. Солонович. Минск : УО «ВА РБ», 2020. – С. 267–269.

3.Утин, Л. Л. К вопросу совершенствования систем охраны протяженных периметров : мат-лы респ. науч.-практич. конф. «Обеспечение пограничной безопасности и охрана государственной границы Республики Беларусь: Теория и практика», Минск, 19 февраля 2020 г. / Л. Л. Утин [и др.]. – Минск : УО «ИПС», 2020.

УДК 004.056

ПРЕДЛОЖЕНИЯ О РАСШИРЕНИИ ТРЕБОВАНИЙ К ЗАЩИТЕ ВИРТУАЛЬНЫХ ИНФРАСТРУКТУР

Н.В. МОЗОЛИНА
Аспирант, МФТИ (НИУ), преподаватель кафедры защиты информации ФРКТ МФТИ, начальник отдела программирования СЗИ, ЗАО «ОКБ САПР»

Технология виртуализации не нова [1], даже атаки, и конечно, защита информационных систем, построенных на этой технологии, имеют свою историю [2]. Так в профессиональных кругах можно встретить мнение, что обеспечение безопасности виртуальных машин, пожалуй, базового объекта в виртуальной инфраструктуре, (ВИ) – это простая инженерная задача с известным решением (например, [3]). Как разработчик средств защиты информации (СЗИ), в том числе для систем виртуализации [4–5], я согласна с этим мнением, но лишь отчасти. В вопросах защиты виртуальных инфраструктур есть аспект, связанный с контролем целостности конфигураций, внимание которому не уделено в должной мере ни регуляторами, ни, зачастую, разработчиками СЗИ. В тоже время сегодня нельзя не заметить появление новых и активное развитие уже существующих отечественных платформ виртуализации и средств защиты для них, а значит, именно сейчас следует пересмотреть настоящие требования к обеспечению безопасности виртуальный инфраструктур и, возможно, усилить их. В данном докладе сфокусируемся на контроле целостности конфигураций виртуальных инфраструктур, и начать разговор о нем хотелось бы с самого понятия целостности. Зачастую в среде специалистов по информационной безопасности можно встретить различные подходы к его определению. Первый звучит следующим образом: «Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право». Согласно второму подходу «целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения)».

Несмотря на противоречивость данных определений (как их самих, так и друг другу), оба зафиксированы в действующих нормативных документах: в [6] и [7] соответственно. Так, в [7] речь идет о целостности информации как о свойстве средства вычислительной техники (СВТ), или, иными словами, свойство информации – это свойство ресурса, хотя информация и СВТ – объекты различной природы. Приведенное же в [6] определение не учитывает, например, что изменения, проведенные субъектами, обладающими соответствующими правами, могут быть хоть и преднамеренными, но преследующими деструктивные цели.

Есть и третий подход: целостность информации как отсутствие ненадлежащих изменений. Смысл понятия “ненадлежащее изменение” раскрывается в [8]: ни одному пользователю информационной, в том числе и авторизованному, не должны быть разрешены такие изменения данных, которые повлекут за собой их разрушение или потерю.

Нельзя не заметить, что в двух из приведенных выше определений целостность определялась для информации, то есть для некоторых данных. И хотя именно данные – это тот объект, защита которого является итоговой целью, но для достижения этой цели могут быть применены два различных подхода: защита собственно данных и защита процессов преобразования и хранения информации, ресурсов программ, обрабатывающих данные, средств вычислительной техники, то есть всего, что можно отнести к информационным ресурсам [9, с. 18]. В сфере обеспечения и контроля целостности, как одном из направлений защиты информации, эти 2 подхода (целостность данных и целостность информационных ресурсов) также выделяются.

В нормативных документах оба подхода закреплены. Например, в действующем ГОСТ «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения» 2016 года можно встретить меры, направленные на защиту дан-

ных («контроль целостности данных, хранимых на машинных носителях информации, подключенных к виртуальной инфраструктуре») и направленные на защиту информационных технологий («контроль целостности микропрограммного обеспечения аппаратной части ИС») [10]. В приказах ФСТЭК № 17 и № 21 2013 года разделение подходов можно увидеть уже в названии одного из блоков мер защиты – «Обеспечение целостности информационной системы и информации» [11, 12], то есть приказы задают меры, направленные на контроль целостности не только данных, но информационных технологий, которые являются неотъемлемой частью информационной системы.

Получается, что сегодня в российской нормативной базе не только нет единства в определении «целостности информации», но и вовсе не закреплено понятие «целостность» применительно к другим объектам защиты, информационным технологиям, хотя оно и используется повсеместно. Несмотря на указанное упущение, – которое, конечно, надлежит исправить, – в профессиональной среде все же есть общее понимание «целостности» в обоих контекстах и достаточные для решения практических задач представления о том, чем эти контексты различаются, что позволяет перейти непосредственно к защите виртуальных инфраструктур.

Возвращаясь к обсуждению контроля целостности конфигураций виртуальных инфраструктур, остановимся на самом понятии конфигурации. Опять же, нормативная база не содержит определения конфигурации, хотя и указывает ее как один из объектов защиты (мера ЗСВ.7 в [11,12]).

Виртуальная инфраструктура состоит из различных компонентов (объектов): виртуальных машин, хостов, хранилищ, сетей, серверов управления и т. д. В зависимости от используемой платформы виртуализации. Каждый из этих объектов обладает набором характеристик (настроек, атрибутов), которые определяют их состояние. Объекты виртуальной инфраструктуры связаны между собой отношениями принадлежности (например, виртуальная машина принадлежит хосту в том смысле, что запущена на нем), управления (например, в рамках решения vSphere кампании VMware возможно управление множеством хостов-гипервизоров ESXi с помощью vCenter Server, передачи данных и т. д. Связи между объектами наряду с их атрибутами определяют функционирование виртуальной инфраструктуры. Таким образом, конфигурация ВИ может быть определена как совокупность множеств объектов, связей между объектами и атрибутами объектов, составляющих информационную систему. Игнорирование обеспечения и контроля целостности любого множества, составляющего конфигурацию ВИ, может привести к возникновению угроз безопасности информационной системы [13, 14].

Подробное описание требований к реализации меры ЗСВ.7 «Контроль целостности виртуальной инфраструктуры и ее конфигураций» приведено в Методическом документе «Меры защиты информации в государственных информационных системах» [15]. Сопоставив приведенные в нем указания с определением конфигурации ВИ и ее контролем целостности, получим таблицу 1. Для каждого требования к реализации и усилению ЗСВ.7 было определено, относится ли оно к контролю целостности объектов, атрибутов объектов или связей между объектами, и в зависимости от этого оно приведено в соответствующем столбце. В некоторых требованиях есть указание по КЦ и самого объекта, и его атрибутов, в таком случае требование указывается сразу с обеих столбцах.

Как видно из таблицы 1, приведенные требования не учитывают контроль целостности связей между объектами виртуальной инфраструктуры. Стоит отметить, что отчасти связь объектов контролируется мерами ЗВС.6 «Управлением перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных», хотя и лишь в отношении виртуальных машин. В связи с этим требование контроля связей между объектами можно рассматривать как усиление меры КЦ виртуальной инфраструктуры.

Также таблица 1 показывает, что меры защиты не учитывают контроль атрибутов таких объектов, как хостовая операционная система, гипервизор, сервер и консоль управления виртуализацией. Эти объекты играют ключевую роль в построении и функционировании ВИ, а потому контроль их настроек необходим.

Таблица 1

Сопоставление требований к реализации меры ЗСВ.7 и требований к контролю конфигурации ВИ

Контроль целостности (КЦ) конфигурации виртуальной инфраструктуры		
КЦ объектов	КЦ атрибутов объектов	КЦ связей между объектами
Требования к реализации ЗСВ.7:		
В информационной системе должен обеспечиваться контроль целостности компонентов виртуальной инфраструктуры в соответствии с ОЦЛ.1		
Контроль целостности компонентов, критически важных для функционирования хостовой операционной системы, гипервизора, гостевых операционных систем и (или) обеспечения безопасности обрабатываемой в них информации (загрузчика, системных файлов, библиотек операционной системы и иных компонентов)		
Контроль целостности состава и конфигурации виртуального оборудования		
	Контроль целостности файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин	
Контроль целостности файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем		
В информационной системе должен обеспечиваться контроль целостности резервных копий виртуальных машин (контейнеров)		
Требования к усилению ЗСВ.7:		
в информационной системе должен обеспечиваться контроль целостности базовой системы ввода-вывода вычислительных серверов и консолей управления виртуальной инфраструктуры		
в информационной системе должен обеспечиваться контроль целостности микропрограмм и служебных данных элементов аппаратной части виртуальной инфраструктуры (в том числе загрузочных записей машинных носителей информации)		
в информационной системе должен обеспечиваться контроль состава аппаратной части компонентов виртуальной инфраструктуры		
в информационной системе должен обеспечиваться контроль целостности программного обеспечения облачных клиентов		

Исходя их приведенных выше рассуждений требования по защите виртуальных инфраструктур, закрепленные в приказах ФСТЭК №17 и №21 [11, 12] и детализированные в Методическом документе «Меры защиты информации в государственных информационных системах» [15], предлагается расширить следующим образом:

- требование к реализации ЗВС.7 дополнить указанием обеспечения контроля целостности компонентов, содержащих настройки функционирования хостовой операционной системы, гипервизора и серверов управления виртуализацией и консолей управления виртуализации;

- требования к усилению меры ЗСВ.7 дополнить указанием, что в информационной системе должен обеспечиваться контроль целостности связей между объектами виртуальной инфраструктуры.

Кроме того, целесообразно зафиксировать в нормативных документах определение целостности, которое может быть применено для произвольного объекта защиты: информации, файла, оборудования, информационной технологии или системы.

Список литературы

1. Fedoseenko, V. A brief history of virtualization, or why do we divide something at all [Электронный ресурс] / V. Fedoseenko. – Режим доступа : https://www.ispsystem.com/news/brief-history-of-virtualization. – Дата доступа : 13.04.2021.
2. Tsifountidis, F. Virtualization security: Virtual machine monitoring and introspection / F. Tsifountidis // Signature [Электронный ресурс]. Режим доступа : https://www.ma.rhul.ac.uk/static/techrep/2011/RHUL-MA-2011-09.pdf. – Дата доступа : 13.04.2021.
3. Как подружить ГОСТ Р 57580 и контейнерную виртуализацию. Ответ Центробанка (и наши соображения на этот счет) [Электронный ресурс] // Блог компании ITGLOBAL.COM. – Режим доступа : https://habr.com/ru/company/itglobalcom/ blog/516102/#comment_21987238. – Дата доступа : 13.04.2021.
4. СПО «Аккорд-KVM». Основные сведения // Официальный сайт ОКБ САПР [электронный ресурс]. URL: https://www.okbsapr.ru/products/virtsys/accord-kvm/main/. – Дата доступа : 11.05.2021.
5. СПО «Аккорд-В.» и «Сегмент-В.». Основные сведения // Официальный сайт ОКБ САПР [электронный ресурс]. – Режим доступа : https://www.okbsapr.ru/products/virtsys/accord-v-and-segment-v/main-segment-v/. – Дата доступа : 11.05.2021.
6. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
7. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Решение председателя Гостехкомиссии России от 30 марта 1992 г.
8. Clark, D. A Comparison of Commercial and Military Computer Security Policies // D. Clark, D. Wilson // IEEE Symposium on Security and Privacy. – P. 184–194.
9. Конявский, В. А. Основы понимания феномена электронного обмена информацией / В. А. Конявский, В. А. Гадасин. – Минск, 2004. – С. 18.
10. ГОСТ Р 56938-2016. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения [Электронный ресурс]. – Режим доступа : http://docs.cntd.ru/document/ 1200135524. – Дата доступа : 30.04.2021.
11. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : Приказ № 17 ФСТЭК России от 11 февраля 2013 г.
12. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : Приказ № 21 ФСТЭК России от 18 февраля 2013 г.
13. Мозолина, Н. В. Контроль целостности виртуальной инфраструктуры и ее конфигураций / Н. В. Мозолина // Комплексная защита информации : мат-лы XXI междунар. конф. – Смоленск, 2016. – С. 167–170.
14. Мозолина, Н. В. Задание эталона при контроле целостности конфигурации виртуальной инфраструктуры / Н. В. Мозолина // Новые Информационные Технологии и Системы : сб. науч. статей XII междунар. науч.-техн. конф., г. Пенза 23–25 нояб. 2016 г. – Пенза, 2017. – С. 219–225.
15. Меры защиты информации в государственных информационных системах : метод. документ ФСТЭК России от 11 февраля 2014 года.

УДК 537.531:621.039.537-037.87

ПРИМЕНЕНИЕ ТЕРМОТРАНСФЕРНОЙ ТЕХНОЛОГИИ ДЛЯ СОЗДАНИЯ УГЛЕРОДОСОДЕРЖАЩИХ ПОГЛОТИТЕЛЕЙ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

Е.С. БЕЛОУСОВА, О.В. БОЙПРАВ, Л.М. ЛЫНЬКОВ
Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Беларусь

Введение. В работах [1–3] представлено обоснование выбора связующего материала для инкорпорирования частиц углерода в волокнистую основу и их закрепления в межволоконном пространстве. По результатам исследования внутренней структуры образцов поглотителей электромагнитного излучения (ЭМИ) с инкорпорированными частицами углерода и частотных зависимостей коэффициентов отражения и передачи в диапазоне частот 0,7–17 ГГц установлено, что эффективным связующим материалом для создания таких поглотителей является нанокомпозит на основе смеси поверхностно-активного вещества и технического углерода. Поглотители электромагнитного излучения на основе синтетического волокнистого материала, на поверхность которого нанесен нанокомпозит на основе смеси поверхностно-активного вещества и технического углерода, характеризуется равномерным распределением в волокнистой основе частиц углерода, что обеспечивает значение коэффициента передачи порядка –18 дБ и коэффициента отражения, равного –12 дБ, в диапазоне частот 7–13 ГГц. Результаты данных исследований получены в ходе серии экспериментов в рамках научно-исследовательской работы государственной программы научных исследований на 2016–2020 годы «Фотоника, опто- и микроэлектроника», подпрограмма «Микро- и наноэлектроника», тематика которой соответствует направлению «Многофункциональные материалы и технологии» Перечня приоритетных направлений фундаментальных и прикладных исследований Республики Беларусь на 2016–2020 годы, утвержденного Постановлением Совета Министров Республики Беларусь от 12 марта 2015 г. № 190.

В рамках научно-исследовательской работы «Разработка радиопоглощающих композиционных структур на основе порошкообразных углесодержащих материалов» по заданию № 1.5 «Разработка новых материалов и технологий для систем электромагнитной защиты радиоэлектронного и информационного оборудования, биологических объектов от воздействия широкого спектра электромагнитных излучений, обеспечения электромагнитной безопасности населения и электромагнитной совместимости электро-, радиотехнических средств и оборудования» ГПНИ «Материаловедение, новые материалы и технологии» на 2021–2025 гг. исследования были продолжены, а именно установлено влияние давления на поверхность и температуры на изменение толщины углеродосодержащих поглотителей ЭМИ.

Для исследования влияния давления и температуры на изменение толщины углеродосодержащих поглотителей ЭМИ сначала были изучены технологии термопереноса, которые используются в полиграфии для нанесения и закрепления красящего состава на поверхность различных видов материалов, в том числе и ткани. К таким технологиям относят термотрансферную и сублимационную технологии.

В технология сублимации используется трафарет, называемый термотрасфером, который представляет собой бумагу с красящим составом. Термотрансфер совмещается с лицевой стороной материала-носителя, на который планируется перенос красящего состава, и помещается под термопресс. Под давлением на поверхность термотрансфера, создаваемым рабочими нагретыми поверхностями пресса происходит процесс термопереноса красящего состава с термотрансфера на материал-носитель за счет чего красящий состав проникает в волокна материала-носителя.

Также существует технология прямой сублимации, которая основа на нанесение красящего состава непосредственно на материал-носитель под воздействием высоких температур без использования термотрансферов. В данной технологии красящий состав испаряется под действием высоких температур и проникает в структуру материала-носителя. Недостатком данного метода является ограничение его применения для разных типов поверхностей. Рекомендуется использовать данную технологию только для полиэстеровых, композитных тканей с содержанием полиэстера от 65 % и более [4].

На сегодняшний день наиболее распространенной является термотрансферная технология [5], которая также основана на использовании термотрасфера, красящий состав с поверхности которого переноситься на поверхность материала-носителя под действием высоких температур (160–180 ºС) в течение нескольких секунд и равномерного давления на поверхность термотрасфера и материал-носитель нагретыми рабочими поверхностями пресса. В качестве термотрансфера обычно используют специальные пленки, которые под действием высоких температур способствуют хорошей адгезии красящего состава с поверхностью носителя, устойчивости нанесенного состава к деформации и его долговечности.

На основе изученных технологий термопереноса, можно сделать вывод, что использование термопресса обеспечивает высокую температуру и равномерное давление на поверхность материала, что обеспечивает проникновение в структуру данного материала красящего состава. Поэтому было предложено усовершенствовать методику инкорпорирования частиц аллотропных форм углерода в волокнистый материал и их закрепления в волокнистой матрице для изготовления поглотителей электромагнитного излучения, представленную в [1], посредством добавления этапа обработки поглотителя при в термотрансферном планшетном прессе.

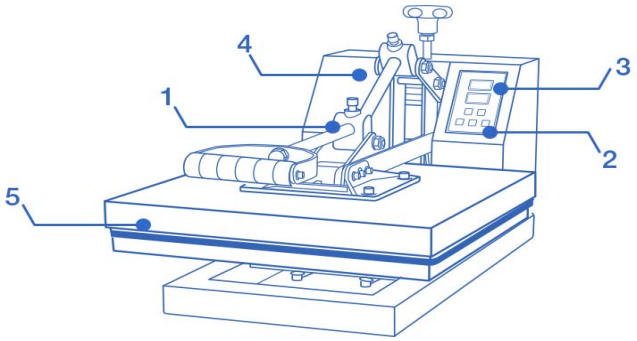


Рис. 1. Внешний вид термотрансферного планшетного пресса:
1 – ручка открытия и закрытия верхней плиты термопресса; *2* – кнопочная панель для настройки таймера;
3 – дисплей отображения времени;
4 – кнопочная панель для настройки температуры;
5 – верхняя плита термопресса

Таким образом, предлагается следующая методика для изготовления углеродосодержащих поглотителей электромагнитного излучения:

1. Приготовление углеродосодержащего нанокомпозита:

– подготовка углеродного порошка (помол, промывка, сушка);

– подготовка композита на основе поверхностно-активного вещества;

– смешивание в равных объемных долях углеродного порошка и композита.

2. Раскрой волокнистого материала (синтетическое нетканное полотно) на фрагменты требуемых размеров и формы.

3. Нанесение на поверхность фрагмента волокнистого материала углеродосодержащего нанокомпозита.

4. Сушка волокнистого материала при температуре 20 ºС в течение 24 часов.

5. Помещение волокнистого материала в термотрансферный планшетный пресс на 10 мин.;

6. Извлечение фрагментов волокнистого материала из термотрансферного планшетного пресса и их охлаждение при стандартных условиях.

По представленной выше методике было изготовлено 3 образца углеродосодержащих поглотителей, каждый помещался в термотрансферный планшетный пресс на 10 минут при разных температурах (50 ºС, 150 ºС, 200 ºС). Сравнительный микроскопический анализ, проведенный с помощью бесконтактного видеоизмерительного микроскопа Norgau NVM-2010,

показал уплотнение синтетических волокон в структуре нетканого полотна и перераспределение углеродных частиц в волокнистой матрице. Также необходимо отметить, что толщина образца уменьшилась на 1–2 мм, и составила 2 мм.

Заключение. Таким образом, усовершенствованная методика изготовления углеродосодержащих поглотителей электромагнитного излучения посредством инкорпорирования частиц углерода в волокнистую матрицу нетканого синтетического волокна обеспечивает уплотнение синтетических волокон и перераспределение углеродных частиц в волокнистой матрице, а также уменьшение толщины поглотителя на 1–2 мм за счет использования в разработанной методике термотрансферного планшетного пресса. Необходимо отметить, что при этом сохраняются свойства гибкости и прочности углеродосодержащего поглотителя электромагнитного излучения.

Несомненно воздействие высокой температуры и давления, а также уменьшение толщины углеродосодержащих поглотителей, изготовленных по представленной в данной работе методике, приведет к изменению частотных зависимостей коэффициентов отражения и передачи, что и планируется реализовать в продолжении научно-исследовательской работы «Разработка радиопоглощающих композиционных структур на основе порошкообразных углесодержащих материалов».

Список литературы

1. Belousova, E. S. Justification of binder material selection for carbon particles incorporation into fibrous electromagnetic radiation absorber / E. S. Belousova, B. I. Dumchev, M. S. Kh. Al-Mahdawi // Доклады БГУИР. – 2020. – № 18 (6). – С. 83–93.

2. Белоусова, Е. С. Экспериментальное обоснование способа получения гибких экранов электромагнитного излучения, основанного на инкорпорировании углерода аллотропных форм в волокнистые матрицы / Е. С. Белоусова, М. С. Х. Аль-Махдави, О. В. Бойправ // Вестник Полоцкого государственного университета. Сер. С, Фундаментальные науки. – 2019. – № 12. – С. 15–20.

3. Белоусова, Е. С. Гибкие экраны электромагнитного излучения на основе углеродосодержащих клеевых составов / Е. С. Белоусова [и др.] // Доклады БГУИР. – 2017. – № 8 (110). – С. 73–78.

4 Преимущества и недостатки сублимационной печати « [Электронный ресурс] – Режим доступа : https://www.mysub.ru/staty/preimnedossublpech.

5 Технология термотрансферной печати / ООО «Термомарк» [Электронный ресурс] – Режим доступа : https://tmark.ru/spravochnik/tehnologiya-termotransfernoy-pechaty/.

УДК 004.56

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ВОЗМОЖНОСТЕЙ МЕТОДА РЕЗОНАСНО-РЕФЛЕКТОМЕТРИЧЕСКОЙ ЛОКАЦИИ ДЛЯ ПОИСКА ЗАКЛАДНЫХ РАДИОУСТРОЙСТВ

А.И. МАЙОРОВ, М.А. БУНЕВИЧ, В.А. ГАВРУКОВИЧ, И.А. ВРУБЛЕВСКИЙ
Органы пограничной службы Республики Беларусь, в/ч 2007, г. Минск, Республика Беларусь,
УО «Белорусский государственный университет информатики и радиоэлектроники»,
г. Минск, Республика Беларусь

Введение. В настоящее время среди средств негласного съема информации наибольшее распространение получили закладные радиоустройства. Этому способствует ряд причин. Во-первых, простота установки и съема информации без необходимости применения сложного оборудования: необходимо лишь само закладное радиоустройство и приемник для приема радиосигналов. Во-вторых, возможность получения информации из первых рук в режиме реального времени [1].

С точки зрения поиска, закладное радиоустройство имеет ряд отличительных признаков. Наиболее характерным является то, что сигнал от закладного устройства должен излучаться за пределы контролируемого помещения и, если оно установлено в этом помещении, то уровень сигнала в нем всегда выше, чем за пределами.

Наиболее доступным методом поиска средств съема информации является простой визуальный осмотр. В настоящее время для поиска закладных устройств применяют специальные поисковые технические средства. Основным методом поиска закладных радиоустройств является контроль радиоэфира с помощью различных радиоприемных устройств. Это различные детекторы диктофонов, индикаторы поля, частотомеры, сканирующие приемники, анализаторы спектра, а также программно-аппаратные комплексы контроля, которые автоматизируют работу перечисленных устройств. Для противодействия перехвату излучения закладных радиоустройств в них сокращают время выхода в радиоэфир.

Повысить вероятность обнаружения закладного устройства можно используя методы поиска по вещественным признакам. Считается, что наиболее эффективный из них – поиск с применением принципов нелинейной локации [2].

Целью статьи является рассмотрение возможностей метода рефлекторно-резонансной локации и оценка возможности его применения для поиска закладных радиоустройств.

Описание принципа метода резонансно-рефлектометрической локации. Метод резонансно-рефлектометрической локации состоит в том, чтобы облучать окружающее пространство зондирующими импульсами в диапазоне частот работы закладных радиоустройств (100 МГц…6 ГГц) и принимать отраженные сигналы.

Основное уравнение радиолокации имеет вид:

$$P_{np} = \frac{P_t G_t A_r \sigma}{(4\pi)^2 D}, \qquad (1)$$

где P_{np} – мощность сигнала на входе приемника; P_t – мощность радиопередатчика; G_t – коэффициент усиления передающей антенны; A_r – эффективная площадь антенны; σ – эффективная отражающая поверхность; D – расстояние от цели до локатора.

Так как закладные радиоустройства имеют малые габариты, их эффективная отражающая поверхность (далее – ЭОП) сравнима с длиной волны зондирующих сигналов. Простейшим примером таких целей в радиолокации является полуволновой вибратор. При равенстве длины вибратора l целому числу полуволн наступает резонанс наведенного тока. Зависимость ЭОП от величины l/λ представлена на рисунке 1 [3].

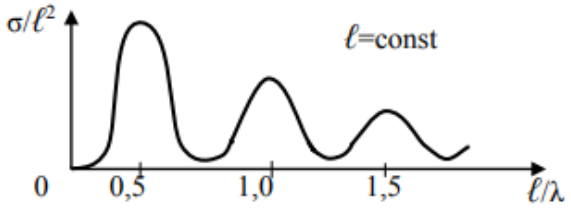


Рис. 1. Зависимость ЭОП от величины l/λ

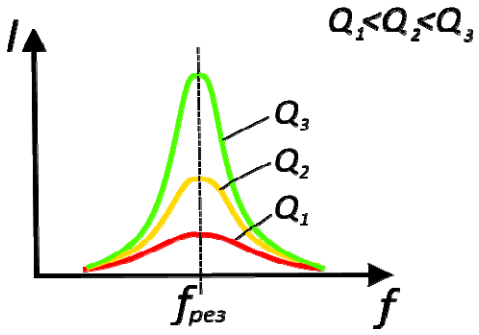


Рис. 2. Обобщенная зависимость наведенного тока в колебательном контуре от частоты и добротности контура

Таким образом, при изменении частоты зондирующего сигнала будет изменяться ЭОП закладного радиоустройства: при совпадении частоты зондирующего сигнала с резонансной частотой колебательного контура антенной системы закладного радиоустройства ЭОП, а, согласно (1), и мощность отраженного сигнала на входе приемника локатора значительно увеличивается.

Большинство закладных радиоустройств работают на фиксированной частоте или в узком диапазоне частот. Для антенных систем таких устройств характерна высокая добротность. Обобщенная зависимость наведенного тока в колебательном контуре от частоты и добротности контура представлена на рисунке 2. Таким образом, при облучении устройств с высокодобротным контуром зондирующим сигналом с частотой, равной резонансной частоте контура, амплитуда наведенных токов в контуре увеличиться пропорционально добротности контура, что также приведет к увеличению мощности сигнала на входе приемника локатора.

Таким образом, можно сделать вывод, что резкое увеличение мощности принятого сигнала при перестройке частоты локатора может свидетельствовать о нахождении в области излучения радиотехнического средства [4].

Сравнение возможностей методов нелинейной локации и резонансно-рефлектометрической локации для задачи поиска закладных радиоустройств. Проведена качественная оценка эффективности обнаружения различных радиоустройств нелинейными локаторами «КАТРАН» и ЛОРНЕТ «СТАР», а также прототипом резонасно-рефлектометрического локатора.

С помощью этих приборов был осуществлен поиск имитаторов закладных радиоустройств. Места установки радиоустройств были заведомо известны. Поиск проводился на различных расстояниях (5–30 см) от радиоустройств. Эксперимент проводился в офисном здании в городской черте в условиях умеренного индустриального электромагнитного шума и помех, вызванных действующими электронными приборами.

В роли имитаторов закладных радиоустройств использовались: мобильный 3G WiFi роутер HUAWEI E5330 (устройство 1), радиореле Intro 7522, работающее на частоте 433,24 МГц (устройство 2), имитатор закладного устройства, работающего на частоте 434 МГц (устройство 3), имитатор закладного устройства, работающего на частоте 1575 МГц (устройство 4).

Имитаторы закладных радиоустройств представляют собой печатную плату с размещенными на ней компонентами беспроводных систем: приемопередатчик, фильтры, антенна, соответствующая диапазону. Все компоненты, кроме антенны, расположены с одной стороны платы под электромагнитным экраном со съемной крышкой. Обратная сторона печатных плат полностью металлизирована. В эксперименте принимали участие также имитаторы с демонтированным электромагнитным экраном (устройства 5 и 6 соответственно). Внешний вид имитаторов представлен на рисунке 3.

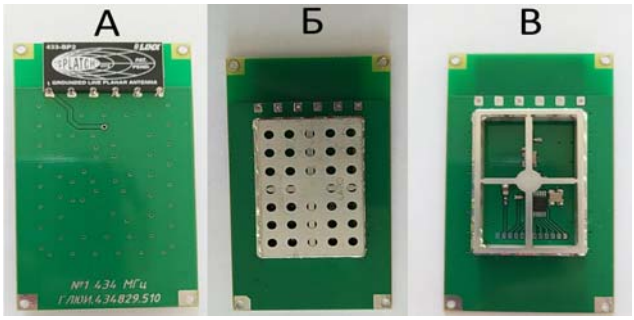


Рис. 3. Внешний вид имитатора закладного радиоустройства, работающего на частоте 434 МГц: *а* – Верхний слой печатной платы с антенной; *б* – нижний слой печатной платы с установленным экраном; *в* – нижний слой печатной платы без экрана

Для каждого радиоустройства было предпринято 10 попыток обнаружения. Устройство считалось обнаруженным, если из 10 попыток обнаружения по крайней мере 6 были успешными. Результаты эксперимента для расстояний *r* от поискового прибора до радиоустройства 5 см, 10 см, 20 см, 30 см сведены в таблицу 1. В таблице приняты следующие условные обозначения: если на заданном рас-

стоянии обнаружить радиоустройство удалось данным поисковым прибором удалось – на пересечении радиоустройства и поискового прибора в таблице «+», если не удалось – «-».

3G WiFi модем и радиореле (устройства 1 и 2 в табл. 1) уверенно обнаруживались на расстояниях больше 30 см всеми исследуемыми поисковыми приборами.

Таблица 1

Результаты эксперимента

Поисковый прибор	Устройство 1	Устройство 2	Устройство 3	Устройство 4	Устройство 5	Устройство 6
r = 5 см						
Нелинейный локатор «КАТРАН»	+	+	-	-	+	-
Нелинейный локатор ЛОРНЕТ «СТАР»	+	+	-	-	+	+
Резонансно-рефлектометрический локатор	+	+	+	+	+	+
r = 10 см						
Нелинейный локатор «КАТРАН»	+	+	-	-	+	-
Нелинейный локатор ЛОРНЕТ «СТАР»	+	+	+	-	+	+
Резонансно-рефлектометрический локатор	+	+	+	+	+	+
r = 20 см						
Нелинейный локатор «КАТРАН»	+	+	-	-	-	-
Нелинейный локатор ЛОРНЕТ «СТАР»	+	+	-	-	-	-
Резонансно-рефлектометрический локатор	+	+	+	+	+	+
r = 30 см						
Нелинейный локатор «КАТРАН»	+	+	-	-	-	-
Нелинейный локатор ЛОРНЕТ «СТАР»	+	+	-	-	-	-
Резонансно-рефлектометрический локатор	+	+	+	+	+	+

Имитаторы закладных устройств на частотах 433 МГц и 1575 МГц со снятой крышкой электромагнитного экрана (устройства 5 и 6 соответственно в таблице 1) нелинейными локаторами уверенно удалось обнаружить на расстоянии 5 см. На расстоянии 10 см уверенное обнаружение обеспечивал только прототип резонансно-рефлектометрического локатора. Нелинейными локаторами на данном расстоянии был обнаружен только имитатор на 433 МГц. На расстояниях свыше 10 см обнаружить устройства 5 и 6 удалось обнаружить только прототипом резонансно-рефлектометрического локатора.

Имитаторы закладных устройств на частотах 433 МГц и 1575 МГц с электромагнитным экраном (устройства 3 и 4 соответственно в таблице 1) нелинейными локаторами уверенно обнаружить не удалось. На расстояниях свыше 5 см уверенное обнаружение обеспечивал только прототип резонансно-рефлектометрического локатора.

Стоит отметить, что обнаружить все радиоустройства, участвующие в эксперименте прототипом резонансно-рефлектометрического локатора удалось на расстояниях до 60 см.

Заключение. Из всех существующих на данный момент технических средств негласного съема информации наибольшее распространение получили закладные радиоустройства. Такое широкое применение закладных радиоустройств объясняется высокой мобильностью, малыми размерами, а также высокой автономностью, которая позволяет не зависеть от наличия коммуникаций в помещении, где устанавливается устройство.

В настоящее время разработаны и применяются различные методы обнаружения технических средств негласного съема информации, однако они известны и хорошо изучены злоумышленниками. Это дает им возможность проводить усовершенствование применяемых закладных устройств с целью уменьшения вероятности их обнаружения.

Большинство существующих методов поиска позволяют обнаруживать закладные радиоустройства только в активном состоянии. В работе экспериментально доказана эффективность экранирования полупроводниковых приборов закладных радиоустройств для снижения вероятности обнаружения нелинейным локатором.

Метод поиска радиоустройств с применением резонансно-рефлектометрической локации базируется на утверждении, что в составе любого закладного радиоустройства имеется антенная система. Для нормальной работы закладного радиоустройства необходимо, чтобы работе антенной системы не мешали экранирующие либо другие конструкции, которые могут применяться для уменьшения вероятности обнаружения закладного устройства. Поскольку антенная система по определению усиливает сигнал на определенной частоте, то, облучая устройство зондирующими импульсами на резонансной частоте антенной системы, можно добиться особенного отклика на входе приемника радиолокатора. Такой отклик будет значительно больше, чем отклики от зондирующих сигналов на других частот. Наличие такого отклика будет являться признаком нахождения в облучаемом пространстве антенной системы радиотехнического устройства.

В работе представлены результаты экспериментов по оценке эффективности метода нелинейной локации и резонансно-рефлектометрической для поиска закладных радиоустройств. Результаты эксперимента показывают эффективность обоих методов в случае поиска закладных радиоустройств, в которых не применяется экранирование полупроводниковых приборов и неэффективность метода нелинейной локации в случае применения экранированных закладных радиоустройств по сравнению с методом резонансно-рефлектометрической локации. С помощью прототипа поискового прибора, работающего по принципу резонансно-рефлектометрической локации, удалось обнаружить имитатор экранированного закладного радиоустройства на расстоянии до 60 см, в то время как дальность обнаружения такого устройства нелинейным локатором составила только 5 см.

Рассмотренный в статье перспективный метод поиска закладных радиоустройств лишен основных недостатков поиска, которые имеют системы поиска с помощью детекторов поля, нелинейных локаторов, систем радиомониторинга, тепловизоров и рентгеновских установок. Реализованный на принципах резонансно-рефлектометрической локации поисковый прибор способен обнаруживать закладные радиоустройства, как в активном, так и в выключенном состоянии, и его работа не чувствительна к экранированию корпуса закладного устройства.

Стоит отметить, что данный метод резонасно-рефлектометрический локации предназначен не для замены уже существующих методов поиска закладных радиоустройств, а для дополнения существующих методов, что позволит осуществлять исследование помещений на предмет закладных устройств более эффективно.

Список литературы

1. Бузов, Г. А. Современные типы закладочных устройств и методы борьбы с ними / Г. А. Бузов // Information Security/ Информационная безопасность – 2014. – № 3. – С. 38–40.

2. Торокин, А. А. Инженерно-техническая защита информации : учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности / А. А. Торокин. – М. : Гелиос АРВ, 2005. – 960 с.

3. Гринкевич, А. В. Радиолокация : учеб. пособие / А. В. Гринкевич. – Минск : БГУИР, 2015. – 190 с.

4. Майоров, А. И. Применение метода резонасно-рефлектометрической локации для поиска закладных радиоустройств / А. И. Майоров, М. А. Буневич, И. А. Врублевский // Материалы XXV научно-практической конференции «Комплексная защита информации». – 2020. – С. 43–48.

ЗАСЕДАНИЕ № 2
КРИПТОГРАФИЯ ДЛЯ ГРАЖДАН И ГОСУДАРСТВА

УДК 519.671

КРИПТОЛОГИЯ И СТОХАСТИКА

Ю.С. ХАРИН
Научно-исследовательский институт прикладных проблем математики и информатики, Белорусский государственный университет, г. Минск, Республика Беларусь

Введение. В современных системах комплексной защиты информации важнейшим способом защиты информации является криптографический способ. Он позволяет с гарантированной стойкостью решить следующие четыре главные практические задачи: 1) конфиденциальность; 2) аутентификация источника сообщения; 3) проверка целостности; 4) невозможность отречения от авторства. Криптографический способ базируется на новой науке Криптологии [2], объединяющей Криптографию и Криптоанализ. Криптография – это отрасль математики, в которой разрабатываются модели, методы, алгоритмы и программные средства **математического преобразования информации** в целях сокрытия ее содержания, предотвращения видоизменения или несанкционированного использования; при этом преобразованное сообщение представляет собой хаотическую, чисто случайную последовательность символов. Криптоанализ – раздел математики, в котором разрабатываются модели, методы, алгоритмы и программные средства анализа криптосистемы или ее входных и выходных сигналов с целью извлечения конфиденциальных параметров, включая **открытый текст**. Стохастика – раздел математики, изучающий модели и методы исследования систем и процессов с учетом случайных элементов. Из этих определений видно, что Криптология и Стохастика тесно связаны: Стохастика представляет математический инструментарий для решения задач Криптологии, Криптология стимулирует Стохастику к разработке новых моделей для исследования сложных последовательностей, циркулирующих в криптосистемах. Следует заметить, что впервые на эту связь обратили внимание академик В.А. Котельников и К. Шеннон, разработав математические основы криптографии с помощью стохастических моделей исходного текста, ключа и зашифрованного сообщения. Настоящий доклад посвящен представлению и использованию новых стохастических моделей в криптологии.

1. Проблема «чистой случайности». Многие задачи криптологии (статистическое тестирование криптографических генераторов, статистический криптоанализ, разностный криптоанализ, линейный криптоанализ, криптоатаки по побочным каналам, стеганография) сводятся к задачам различения некоторой зарегистрированной последовательности символов $x_1, x_2, \ldots$ от «чисто случайной» последовательности и оценки величины этого различия.

Математической моделью последовательностей, порождаемых генераторами, а также последовательностей, возникающих в различных узлах СКЗИ, является дискретный временной ряд (ДВР). Дискретный временной ряд (ДВР) – это случайный процесс $x_t \in A$ на вероятностном пространстве $(\Omega, F, \mathbf{P})$ с дискретным временем $t \in \mathbb{T} = \{1, 2, \ldots\}$ и дискретным множеством состояний A мощности $|A| = N$, $2 \le N < +\infty$. Без потери общности полагаем пространство состояний (алфавит) $A = \{0, 1, \ldots, N-1\}$.

В криптологии в связи с Шенноновской теорией совершенных криптосистем большое внимание уделяется так называемому «чисто случайному» ДВР – равномерно распределенной случайной последовательности (РРСП).

РРСП – это последовательность дискретных случайных величин $x_1, x_2, \ldots \in A = \{0, 1, \ldots, N-1\}$, обладающая двумя свойствами [2]:

C_1) для любого числа $n \in \mathbb{T}$ и произвольных индексов $1 < t_1 < \ldots < t_n$ случайные элементы $x_{t_1}, \ldots, x_{t_n}$ независимы в совокупности;

C_2) для любого $t \in \square$ случайная величина x_t имеет равномерное на A распределение вероятностей: $\mathbf{P}\{x_t = i\} = N^{-1}$, $i \in A$.

В настоящее время известно более сотни методов и алгоритмов генерации последовательностей, по своим свойствам приближающихся к РРСП. Еще больше разработано методов статистического тестирования криптографических генераторов, заключающихся в проверке простой гипотезы $H_0 = \{\{x_t\}$ есть РРСП$\}$ против сложной альтернативы $H_1 = \bar{H}_0 = \{$нарушены свойства $C_1,\ C_2\}$.

Проведенный обзор существующих статистических тестов показывает:

1) многие из существующих тестов не ориентированы на проверку главного свойства C_1, а лишь частных случаев свойств C_1, C_2, т. е. частных случаев альтернативы $H_1 = \bar{H}_0$;

2) многие из известных тестов построены «эвристически» и не фиксируют семейство альтернатив H_1;

3) многие тесты не имеют оценок мощности;

4) при включении нескольких тестов в батарею не удается оптимизировать «составной» тест.

В связи с этим актуальна рассматриваемая далее проблема разработки адекватных стохастических моделей для описания отклонений H_1 от модели РРСП, построения статистических тестов для обнаружения и оценивания таких отклонений.

2. Модели ДВР на основе уклонений от s-мерной равномерности и их энтропийный анализ. Определим вложенное в H_1 семейство «альтернатив s-мерной неравномерности»:

$$H_{1(s)} = \{\{x_1, x_2, \ldots\} = \{X_1, X_2, \ldots\}\} \subset H_1,$$

где $X_1, X_2, \ldots \in A^s$ – независимые одинаково распределенные s-фрагменты (слова) над алфавитом A с некоторым s-мерным дискретным распределением вероятностей $\mathbf{P}_{i_1,\ldots,i_s} = \mathbf{P}\{x_1 = i_1, \ldots, x_s = i_s\}$, $i_1, \ldots, i_s \in A$, отличным от равномерного:

$$\Delta_s = \sum_{i_1,\ldots,i_s \in A} \left|\mathbf{P}_{i_1,\ldots,i_s} - N^{-s}\right| > 0, \quad \sum_{i_1,\ldots,i_s \in A} \mathbf{P}_{i_1,\ldots,i_s} \equiv 1.$$

Это семейство моделей ДВР обладает двумя свойствами: 1) при $s \to \infty$ семейство этих альтернатив имеет в пределе альтернативу $H_1 = \bar{H}_0$ общего вида; 2) чем меньше Δ_s, тем ближе альтернатива $H_{1(s)}$ к нулевой гипотезе H_0.

Обозначим: $\{x_1, x_2, \ldots, x_T\} = \{X_1, X_2, \ldots, X_M\}$ – наблюдаемая реализация выходной последовательности длиной $T = M \cdot s$, разбитая на M непересекающихся фрагментов длины s, $I\{B\}$ – индикатор события B,

$$\hat{\mathbf{P}}_{i_1,\ldots,i_s} = \frac{1}{M}\sum_{m=1}^{M} I\{X_m = (i_1, \ldots, i_s)\},\ i_1, \ldots, i_s \in A, - \qquad (1)$$

статистическая оценка для $\mathbf{P}_{i_1,\ldots,i_s}$.

Тест обобщенного отношения правдоподобия для проверки H_0, $H_{1(s)}$ на основе статистик (1) имеет вид:

$$\text{принимается} \begin{cases} H_0, \text{ если } \hat{H}_s - s\ln N > -\dfrac{1}{2M} G^{-1}_{N^s-1}(1-\varepsilon), \\ \qquad H_{1(s)} \text{ в противном случае,} \end{cases} \qquad (2)$$

$$\hat{H}_s = \sum_{i_1,\ldots,i_s \in A} \hat{\mathbf{P}}_{i_1,\ldots,i_s} \ln \hat{\mathbf{P}}_{i_1,\ldots,i_s} -$$

– статистическая оценка s-мерной энтропии Шеннона, $G_K^{-1}(\cdot)$ – обратная функция распределения хи-квадрат с K степенями свободы, $\varepsilon \in (0,1)$ – заданный уровень значимости теста.

Тест (1), (2) мы предлагаем использовать для визуализации процесса принятия решений в виде так называемого «энтропийного профиля (портрета)» – графика зависимости нормированного уклонения оценки s-мерной энтропии от ее математического ожидания при H_0 (см. рис. 1, 2, где штриховые линии обозначают границы области решений):

$$\alpha(s) = 2M\left(\hat{H}_s - s\ln N\right) / G_{N^s-1}^{-1}(1-\varepsilon), \quad s \in \{s_{min}, s_{min}+1, \ldots, s_{max}\}. \tag{3}$$

Отметим еще, что вместо энтропии Шеннона в (1) – (3) могут использоваться энтропийные функционалы Реньи и Тсаллиса [4].

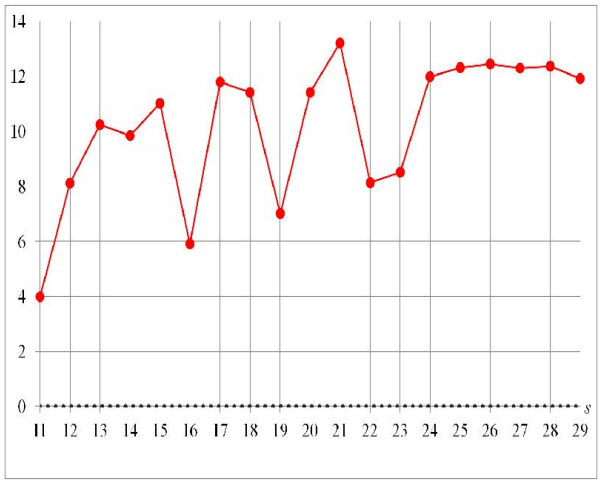


Рис. 1. Энтропийный профиль $\ln|\alpha(s)|$ нелинейного регистра сдвига порядка 24 ($N = 2, \varepsilon = 0.05, T = 2^{32}/s$)

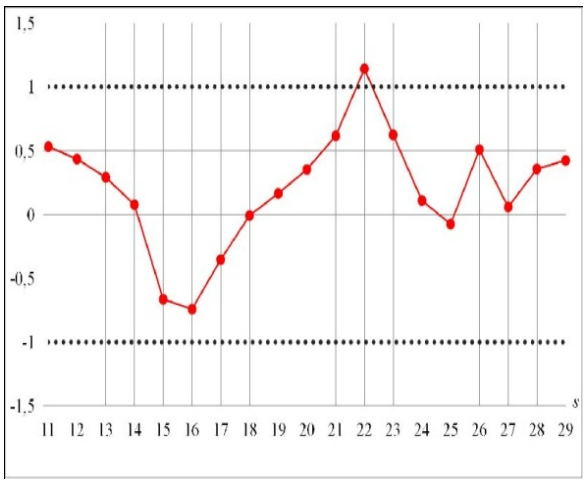


Рис. 1. Энтропийный профиль $\alpha(s)$ генератора BelT (СТБ 34.101.27-2011, $N = 2, \varepsilon = 0.05, T = 2^{29}/s$)

3. Универсальная модель ДВР на основе цепей Маркова высокого порядка. Учитывая, что универсальной моделью стохастической зависимости элементов выходной последовательности $\{x_t\}$ криптографического генератора является цепь Маркова достаточно высокого порядка s, определим вложенное в $H_1 = \bar{H}_0$ семейство альтернатив марковской зависимости: $H_1^{(s)} = \{\{x_t\}$ однородная цепь Маркова порядка s с матрицей переходов $\mathbf{P}\}$, где $\mathbf{P} = \left(p_{i_1,\ldots,i_{s+1}}\right)$, $i_1,\ldots,i_{s+1} \in A - (s+1)$-мерная матрица,

$$p_{i_1,\ldots,i_{s+1}} = \mathbf{P}\{x_{t+1} = i_{s+1} \mid x_t = i_s, \ldots, x_{t-s+1} = i_1\},$$

$$\Delta_s = \sum_{i_1,\ldots,i_s \in A} \left| p_{i_1,\ldots,i_{s+1}} - N^{-1} \right| > 0. \tag{4}$$

Тест обобщенного отношения правдоподобия для проверки гипотез H_0, $H_1^{(s)}$ основан на статистической оценке $\hat{h}_s$ условной энтропии $h_s = H\{x_t \mid x_{t-1}, \ldots, x_{t-s}\}$:

$$\text{принимается} \begin{cases} H_0, \text{ если } \hat{h}_s - \ln N > -G_f^{-1}(1-\varepsilon)/\left(2(T-s)\right), \ f = N^s(N-1), \\ H_1^{(s)} \text{ в противном случае.} \end{cases} \tag{5}$$

Аналогично (3) с помощью $\hat{h}_s$ строится энтропийный профиль для $\{x_1, \ldots, x_T\}$.

К сожалению, тесты (2), (5), анализирующие стохастические зависимости глубины s в выходной последовательности $\{x_t\}$, требуют экспоненциально растущей с ростом порядка s длины анализируемой последовательности $T = O\left(N^{s+1}\right)$. Для преодоления этой трудности целе-

сообразно использовать так называемые «малопараметрические модели цепей Маркова высокого порядка» [1, 2], т. е. модели цепей Маркова s-го порядка, для которых $\left(N^s \times N\right)$-матрица вероятностей переходов зависит от «малого» числа параметров $D \ll N^s\left(N-1\right)$; $\kappa = D/\left(N^s\left(N-1\right)\right) \ll 1$ – коэффициент сжатия, равный относительному числу параметров модели.

4. Подходы к построению малопараметрических цепей Маркова высокого порядка

Подход I. Этот подход состоит в «сжатии множества значений элементов матрицы» $\mathbf{P}$.

Пусть $Q = \left(q_{j_i,\ldots,j_r,j_{r+1}}\right)$ – некоторая $(r+1)$-мерная матрица, $1 \le r < s$,

$$\sum_{j_{r+1} \in A} q_{j_i,\ldots,j_r,j_{r+1}} \equiv 1, 0 \le q_{j_i,\ldots,j_r,j_{r+1}} \le 1;$$

$B(\cdot)\colon A^s \to A^r$ – некоторая дискретная функция. С помощью $B(\cdot)$ $(s+1)$-мерная матрица $\mathbf{P}$ «сжимается» в $(r+1)$-мерную матрицу Q преобразованием:

$$p_{i_1,\ldots,i_s,i_{s+1}} = q_{B(i_1,\ldots,i_s),i_{s+1}};\ \kappa_{\mathrm{I}} = N^{r-s} \le 1. \qquad (6)$$

Примеры малопараметрических ДВР в рамках подхода I: $\mathrm{MC}(s,r)$, $\mathrm{MCCO}(s,L)$, VLMC [5].

Подход II. Этот подход заключается в использовании порождающего уравнения для условного распределения вероятностей (4) будущего состояния $x_t \in A$ при условии предыстории $X_{t-s}^{t-1} = \left(x_{t-1},\ldots,x_{t-s}\right)' \in A^s$:

$$p_{i_1,\ldots,i_s,i_{s+1}} = q_{i_{s+1}}\left(\theta\left(i_1,\ldots,i_s;a\right)\right),\ i_1,\ldots,i_{s+1} \in A, \qquad (7)$$

где $\left\{q_j(\theta)\colon j \in A\right\}$ – некоторое вероятностное распределение на A, зависящее от параметра $\theta = \left(\theta_j\right) \in \Theta \subseteq R^L$; $\theta = \theta\left(i_1,\ldots,i_s;a\right)$ – некоторая функция, известная с точностью до вектора параметров $a = \left(a_k\right) \in R^m$. Коэффициент сжатия:

$$\kappa_{\mathrm{II}} = \frac{m}{N^s\left(N-1\right)} \le 1.$$

Примеры малопараметрических ДВР в рамках подхода II: модель Джекобса – Льюиса, MTD-модель, $\mathrm{DAR}(s)$, $\mathrm{BCNAR}(s)$, $\mathrm{BiCNAR}(s)$, $\mathrm{PCNAR}(s)$.

5. Малопараметрические модели ДВР на основе подхода I и их статистический анализ

Цепь Маркова $\mathrm{MC}(s,r)$ порядка s с r частичными связями. Эта модель определяется формулой (6) с $B\left(j_1\ldots,j_s\right) = \left(j_{m_1^0},\ldots,j_{m_r^0}\right)$ [1, 2]:

$$p_{J_1^{s+1}} = p_{j_1,\ldots,j_s,j_{s+1}} = q_{j_{m_1^0},\ldots,j_{m_r^0},j_{s+1}},\ J_1^{s+1} \in A^{s+1}, \qquad (8)$$

где $J_i^k = \left(j_i, j_{i+1},\ldots,j_k\right) \in A^{k-i+1}$ – последовательность $k-i+1$ индексов $\left(k \ge i\right)$; r – число связей; $M_r^0 = \left(m_1^0,\ldots,m_r^0\right)$ – вектор с r упорядоченными целыми компонентами $1 = m_1^0 < m_2^0 < \ldots < m_r^0 \le s$, называемый шаблоном связей; $Q = \left(q_{J_1^{r+1}}\right)_{J_1^{r+1} \in A^{r+1}}$ – $(r+1)$-мерная стохастическая матрица. Если $r = s$, то получаем полносвязную цепь Маркова порядка s.

Статистическую оценку $\hat{Q}$ удобно использовать для визуализации уклонения от гипотезы H_0 (для которой $q_{i_1,\ldots,i_{r+1}} = N^{-1}$). На рис. 3, 4 представлены результаты такой визуализации для генератора со случайной обратной связью и генератора BelT (СТБ 34.101.27-2011 в режиме гаммирования) соответственно; здесь красный цвет – оценка условной вероятности

перехода в «0» $\hat{q}_{K_1^r,0}$, зеленый – в «1» $\hat{q}_{K_1^r,1}$); здесь по оси абсцисс откладывается $K_1^r = B\left(J_1^s; \hat{M}_r\right) \in A^r$.

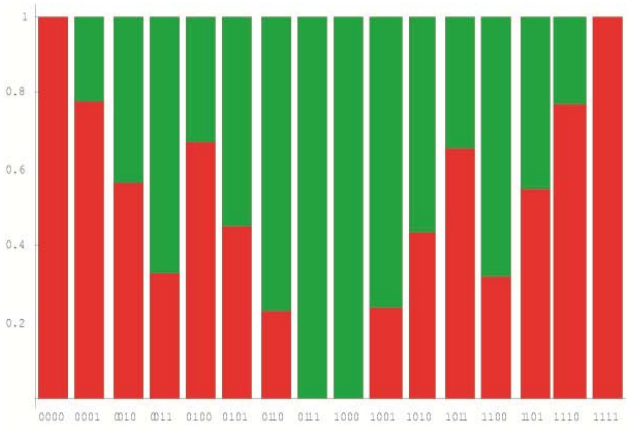


Рис. 3. Оценка $\hat{Q}$ $\left(s=64,\ r=4,\ T=10^5\right)$

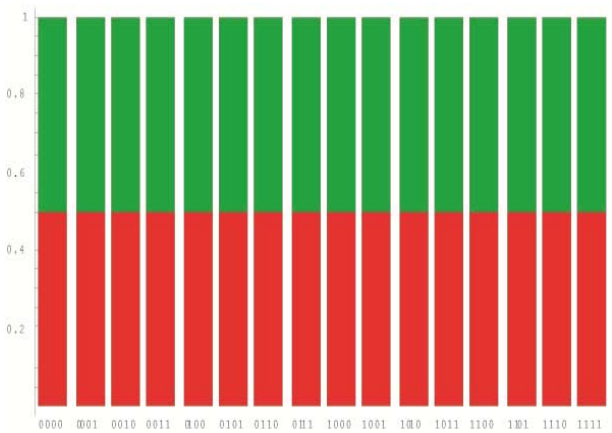


Рис. 4. Оценка $\hat{Q}$ $\left(s=32,\ r=4,\ T=8\cdot 10^6\right)$

С моделью $\mathrm{MC}(s,r)$ связана модель цепи Маркова переменного порядка [5].

6. Малопараметрические модели ДВР на основе подхода II и их статистический анализ

Модель Джекобса – Льюиса. Эта модель порождается стохастическим разностным уравнением [6]:

$$x_t = \mu_t x_{t-\eta_t} + (1-\mu_t)\xi_t, \tag{9}$$

где $t > s$, $\{\xi_t, \eta_t, \mu_t\}$ – независимые в совокупности случайные величины с вероятностными распределениями:

$$\mathbf{P}\{\mu_t = 1\} = 1 - \mathbf{P}\{\mu_t = 0\} = \rho;\ \mathbf{P}\{\xi_t = k\} = \pi_k\ ,\ k \in A\ ,\ \sum_{k\in A}\pi_k = 1\ ;$$

$$\mathbf{P}\{\eta_t = i\} = \lambda_i\ ,\ i \in \{1,2,\ldots,s\}\ ,\ \sum_{i=1}^{s}\lambda_i = 1,\ \lambda_s \neq 0\ ; \tag{10}$$

$$\mathbf{P}\{x_1 = k\} = \ldots = \mathbf{P}\{x_s = k\} = \pi_k\ ,\ k \in A\ .$$

Число параметров этой модели (9), (10) линейно (а не экспоненциально!) зависит от s, так что коэффициент сжатия

$$\kappa_{JL} = (N+s-1)/\left(N^s(N-1)\right).$$

Методы и алгоритмы статистического анализа модели Джекобса – Льюиса представлены в [2].

MTD-модель Рафтери. MTD (Mixture Transition Distribution) – модель [8] определяется следующим частным случаем уравнения (7):

$$p_{i_1,\ldots,i_s,i_{s+1}} = \sum_{j=1}^{s}\lambda_j q_{i_j,i_{s+1}}\ ,\ i_1,\ldots,i_{s+1} \in A\ ,$$

где $Q = \left(q_{i,k}\right)$ – некоторая стохастическая $(N\times N)$-матрица,

$$0 \le q_{i,k} \le 1\ ,\ \sum_{k\in A} q_{i,k} \equiv 1\ ,\ i,k \in A\ ,$$

$\lambda = (\lambda_1,\ldots,\lambda_s)'$ – некоторое дискретное распределение вероятностей, $\lambda_1 > 0$.

Обобщенная MTDg (generalized MTD)-модель определяется следующей параметризацией $(s+1)$-мерной матрицы $\mathbf{P}$:

$$p_{i_1,\ldots,i_s,i_{s+1}} = \sum_{j=1}^{s}\lambda_j q^{(j)}_{i_j,i_{s+1}}\ ,\quad i_1,\ldots,i_{s+1} \in A\ , \tag{11}$$

где $Q^{(j)} = \left(q_{i,k}^{(j)}\right)$ – некоторая стохастическая матрица для j-го лага.

Относительное число параметров MTDg-модели (11):

$$\kappa_{\text{MTDg}} = \left(s\left(N\left(N-1\right)/2+1\right)-1\right)/\left(N^s\left(N-1\right)\right).$$

Биномиальная условно нелинейная авторегрессионная модель BiCNAR(s). Эта модель порождается специальным (биномиальным) случаем порождающего уравнения (7):

$$p_{i_1,\ldots,i_s,i_{s+1}} = C_{N-1}^{i_{s+1}}\ \theta^{i_{s+1}}\left(1-\theta\right)^{N-1-i_{s+1}},\ i_{s+1} \in A = \left\{0,1,\ldots,N-1\right\},$$

$$\theta = \theta\left(\mathrm{I}_1^{\mathrm{s}}\right) = \mathrm{F}\left(a'\Psi\left(\mathrm{I}_1^{\mathrm{s}}\right)\right),\ \mathrm{I}_1^{\mathrm{s}} = \left(i_1,\ldots,i_s\right)' \in A^s,$$

где $\Psi\left(\mathrm{I}_1^{\mathrm{s}}\right) = \left(\psi_1\left(\mathrm{I}_1^{\mathrm{s}}\right),\ldots,\psi_m\left(\mathrm{I}_1^{\mathrm{s}}\right)\right)'$: $A^s \to R^m$ – вектор-столбец $m \le N^s$ линейно независимых функций, например, полиномов; $\mathrm{F}(\cdot)$: $R^1 \to [0,1]$ – некоторая функция распределения, например, логистическая, нормальная или Коши:

$$\Lambda(\zeta) = \frac{1}{1+e^{-\zeta}},\ \Phi(\zeta) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\zeta} e^{-\frac{x^2}{2}}dx,\ C(\zeta) = \frac{1}{2} + \frac{\arctan(\zeta)}{\pi},\ \zeta \in R^1;$$

$a = \left(a_1,\ldots,a_m\right)'$ – вектор-столбец m неизвестных параметров модели.

Относительное число параметров модели: $\kappa = m\left(N^s\left(N-1\right)\right)^{-1} < 1$.

Методы и алгоритмы статистического анализа BiCNAR(s)-модели, ее частных случаев и обобщений представлены в [3, 7].

Заключение. В криптологии актуальна проблема построения и статистического анализа моделей дискретных временных рядов, адекватно описывающих отклонения от модели РРСП.

1. В статье представлены такие семейства моделей ДВР на основе уклонений от s-мерной равномерности и на основе цепей Маркова порядка s.

2. Для преодоления «проклятия размерности» представлены два подхода к построению малопараметрических моделей цепей Маркова высокого порядка.

3. Разработаны методы и алгоритмы статистического анализа (оценивание параметров, проверка гипотез) малопараметрических моделей, построенных на основе предложенных подходов.

4. Теоретические результаты иллюстрируются результатами компьютерных экспериментов по тестированию выходных последовательностей известных криптографических генераторов.

Список литературы

1. Харин, Ю. С. Цепи Маркова с s-частичными связями и их статистическое оценивание / Ю. С. Харин // Доклады НАН Беларуси. – 2004. Т. 48, № 1, с. 40 – 44.

2. Харин, Ю. С. Криптология / Ю. С. Харин [и др.]. – Минск: БГУ, 2014.

3. Харин, Ю. С. Биномиальные условно нелинейные авторегрессионные модели дискретных временных рядов и их вероятностные и статистические свойства / Ю. С. Харин, В. А. Волошко // Труды Института Математики НАН Беларуси. – 2019. – Т. 26, № 1. – С. 95–105.

4. Харин, Ю. С. Энтропийный анализ криптографических генераторов случайных и псевдослучайных последовательностей / Ю. С. Харин, В. Ю. Палуха // Веснік сувязі. – 2017. – Т. 146, № 1. – С. 46–49.

5. Buhlmann, P. Variable length Markov chains. / P. Buhlmann, A. J. Wyner // The Annals of Statistics. – 1999. – Vol. 27, No. 2. – P. 480–513.

6. Jacobs, P. A. Discrete time series generated by mixtures I: correlational and runs properties. / P. A. Jacobs, P. A. W. Lewis // Journal of the Royal Statistical Society. Ser. B. – 1978. – Vol. 40, No. 1. – P. 94–105.

7. Kharin, Yu. S. Statistical estimation of parameters for binary conditionally nonlinear autoregressive time series / Yu. S. Kharin, V. A. Voloshko, E. A. Medved // Mathematical Methods of Statistics. – 2019. – Vol. 26, No. 2. – P. 103–118.

8. Raftery, A. A model for high-order Markov chains / A. Raftery // Journal of the Royal Statistical Society. Ser. B. – 1985. – Vol. 47, No. 3. – P. 528–539.

УДК 004.056

БЕЛОРУССКАЯ ИНТЕГРИРОВАННАЯ СЕРВИСНО-РАСЧЕТНАЯ СИСТЕМА И ВНЕДРЕНИЕ ID-КАРТ

Д.В. МОСКАЛЕВ
Республиканское унитарное предприятие «Национальный центр электронных услуг», г. Минск, Республика Беларусь

Белорусская интегрированная сервисно-расчетная система (БИСРС) – комплекс информационных систем и ресурсов, предназначенный для идентификации пользователей (физических и юридических лиц) с применением идентификационных карт (ID-карт) в целях оказания им электронных услуг (в т.ч. административных процедур).

Создание БИСРС – важный шаг в развитии электронного правительства, который станет следующим звеном между гражданами, бизнесом и государством в цифровом мире. БИСРС облегчит и упростит диалог путем уменьшения бюрократических требований для оказания электронных услуг и пересмотра своих внутренних процессов с учетом применения современных цифровых решений.

БИСРС состоит из следующих компонентов:

В рамках создания БИСРС были решены следующие задачи:

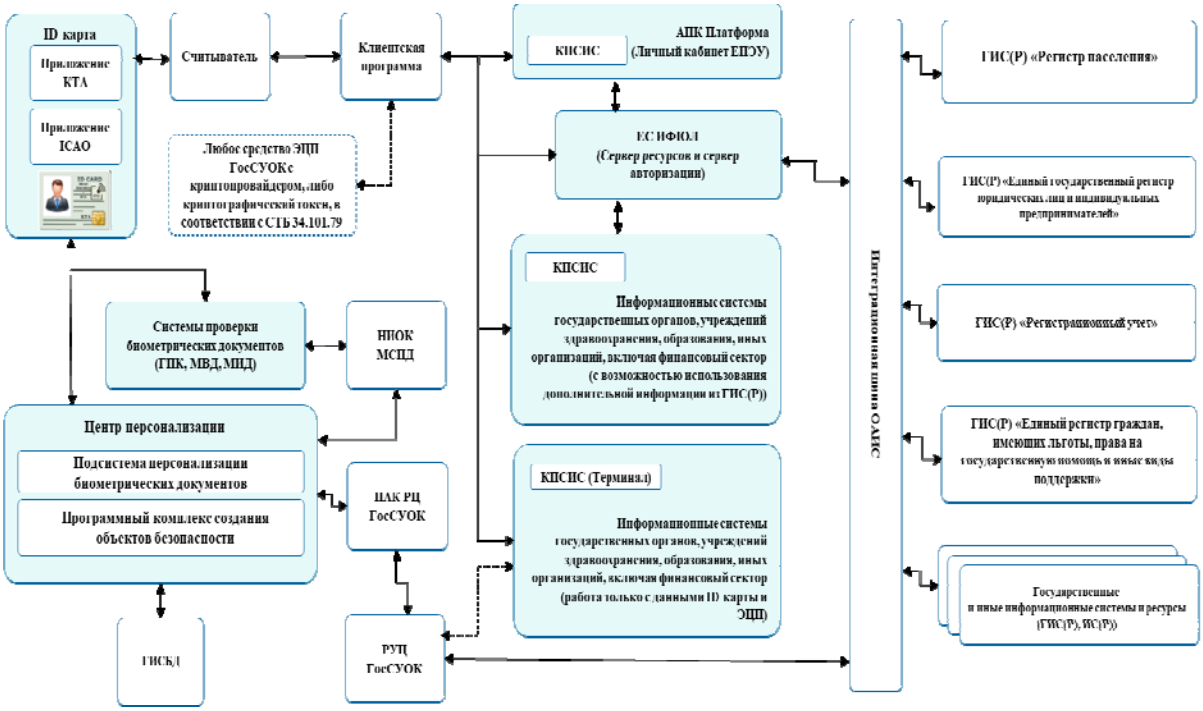
1. Разработана Единая система идентификации физических и юридических лиц (ЕС ИФЮЛ).
2. Создана Национальная инфраструктура открытых ключей машиносчитываемых проездных документов (НИОК МСПД).
3. Проведена модернизация (развитие) и создание ГИС и ГИР, являющихся поставщиками данных БИСРС.
4. Выполнена работа «Разработка криптографического токена аутентификации на идентификационной карте» (программный комплекс «Криптографический токен аутентификации для идентификационной карты», программный комплекс создания объектов безопасности КТА).
5. Создан Центр персонализации биометрических документов.
6. Создана системы сбора и обработки биометрических данных, персонализации, выдачи и контроля биометрических документов, обеспечивающих удостоверение личности гражданина и его идентификацию (ГИСБД).

Одной из базовых компонент БИСРС является Единая система идентификации физических и юридических лиц (далее – ЕС ИФЮЛ).

ЕС ИФЮЛ разрабатывалась в рамках исполнения ОКР «Разработка компонентов Белорусской интегрированной сервисно-расчетной системы (Единая система идентификации физических и юридических лиц, Клиентская программа)» по мероприятию 12 «Создание Белорусской интегрированной сервисно-расчетной системы» (Этап 2 – Создание информационно-коммуникационной инфраструктуры Белорусской интегрированной сервисно-расчетной системы (внедрение пилотной зоны)) подпрограммы 2 «Инфраструктура информатизации» Государственной программы развития цифровой экономики и информационного общества на 2016–2020 годы (в редакции постановления Совета Министров Республики Беларусь от 9 ноября 2018 г. № 806).

Исполнитель ОКР – научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации» (государственное предприятие «НИИ ТЗИ»).

Целью выполнения ОКР явилось формирование единых подходов к обеспечению идентификации гражданина с использованием информационно-коммуникационных технологий и обеспечение юридически значимого электронного взаимодействия между гражданами и государством (за счет реализации возможности совершения юридически значимых действий посредством электронной цифровой подписи (ЭЦП)).



Для достижения цели были решены следующие задачи:

а) разработаны базовые и иные компоненты Белорусской интегрированной сервисно-расчетной системы (БИСРС):

1) программное обеспечение Единой системы идентификации физических и юридических лиц (далее – ЕС ИФЮЛ);

2) клиентскую программу (КП);

б) проведены мероприятия по проектированию и созданию системы защиты информации (СЗИ) ЕС ИФЮЛ;

в) обеспечено сопряжение ЕС ИФЮЛ с государственной информационной системой (ГИС) «Регистр населения», автоматизированной информационной системой (АИС) «Единый государственный регистр юридических лиц и индивидуальных предпринимателей», АИС «Государственный реестр плательщиков (иных обязанных лиц)».

ID-карта. Основным документом, удостоверяющим личность гражданина на территории Республики Беларусь, будет являться ID-карта (в том числе биометрический вид на жительство в Республике Беларусь иностранного гражданина).

ID-карта в своем составе содержит интегральную микросхему (чип), на которую записываются два приложения:

- криптографический токен аутентификации (КТА) – программное обеспечение с информацией о владельце (в соответствии с белорусскими стандартами) и для выработки ЭЦП, сертификат открытого ключа (СОК), изданный в ГосСУОК. КТА содержит два компонента: приложение eSign и приложение eID;

- программное обеспечение, соответствующее требованиям ИКАО с информацией о владельце в международном формате.

На КТА в приложение eSign записываются два СОК физического лица (стандартный (предназначенный для использования в локальном режиме) и терминальный (для использования при работе в удаленном (терминальном) режиме)). Кроме того, для обеспечения доступа к защищаемым персональным данным в чипе ID-карты в режиме считывания данных на КТА записывается СОК корневого удостоверяющего центра облегченных сертификатов Республики Беларусь.

Для выполнения процедуры идентификации/аутентификации и выработки ЭЦП в ЕС ИФЮЛ используется программный КТА, реализуемый в виде криптографического приложения на ID-карте, секретом которого должен быть криптографический ключ (личный или секретный), а аутентификатором – ЭЦП.

Для обеспечения доверия данных в биометрических документах в соответствии с требованиями ИКАО, а также для поддержки механизмов защиты данных, хранящихся в МСПД, создана НИОК. НИОК обеспечивает доверие к данным, содержащимся в МСПД в части верификации ЭЦП, выработанных на объектах МСПД, включая объект защиты документа, для подтверждения того, что подписанные данные являются аутентичными и не изменены.

НИОК представляет собой иерархическую систему, состоящую из следующих компонентов:

CSCA (Country Signing Certification Authorities) – корневой удостоверяющий центр для издания СОК должностным лицам, подписывающим объекты защиты МСПД;

DS (Document Signer) – сервис подписи документов, выполняющий функции создания запроса в CSCA для издания и выдачи СОК DS и выработки ЭЦП для LDS, записываемых на чип МСПД;

CVCA (Country Verifying Certification Authorities) – корневой удостоверяющий центр для издания СОК, обеспечивающих управление доступом к проверке электронных документов уполномоченными органами;

DV (Document Verifier) – подчиненный для CVCA удостоверяющий центр для подразделений уполномоченных органов по проверке документов, издающий СОК для центра (центров) управления терминалами, которые используются для проверки подлинности МСПД;

TCC (Terminal Control Center) – центр управления терминалами, выполняющий функции IS для доступа к защищаемым персональным данным в чипе МСПД с использованием механизмов EAC;

NPKD (National Public Key Directory), НД – национальная директория открытых ключей для централизованного хранения СОК, изданных в НИОК, и взаимодействия с ИКАО и внутренними потребителями.

Схема взаимодействия компонентов НИОК представлена на рисунке 1.

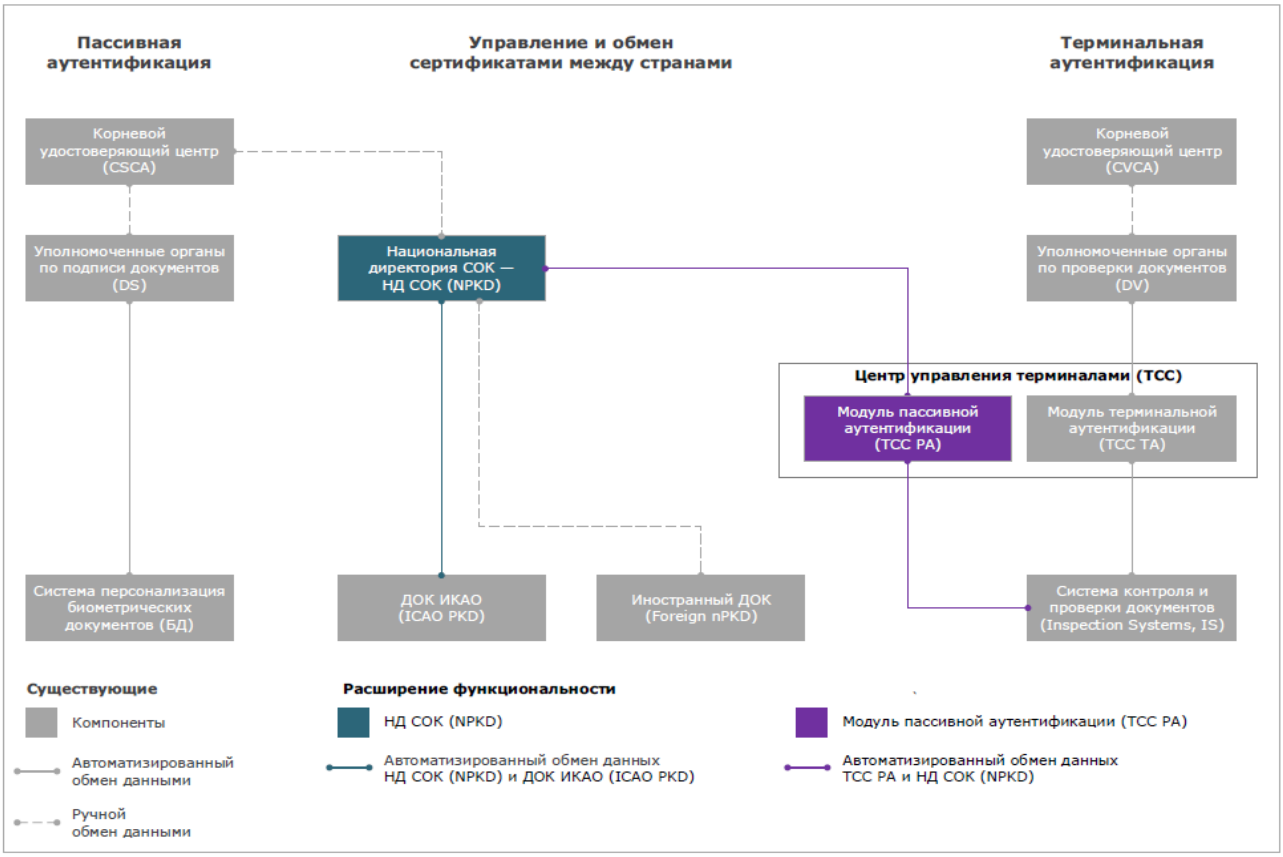


Рис. 1. Схема взаимодействия компонентов НИОК

Переход к использованию в МСПД электронных и биометрических технологий значительно повышает их защищенность от подделок и обеспечивает гарантированную идентификацию их владельцев.

В ПО ИКАО импортируются корневые СОК CSCA и CVCA. С помощью DS осуществляется выработка ЭЦП для LDS, записываемых на чип МСПД.

ЕС ИФЮЛ и КП. ЕС ИФЮЛ предназначена для предоставления информационным системам различных государственных органов и организаций Республики Беларусь сервиса идентификации/аутентификации.

ЕС ИФЮЛ обеспечивает предоставление прикладным системам (ПС) сервисов аутентификации и авторизации, реализованных на основе спецификации OpenID connect (OIDC) с использованием криптографических алгоритмов, определенных в СТБ.

Пользовательская система (ПС) – это зарегистрированная в ЕС ИФЮЛ информационная система, которая организует авторизацию пользователя и предоставляет доступ к своим ресурсам.

Клиентская программа (КП) предназначена для организации взаимодействия между пользователем, его КТА на ID-карте или средства ЭЦП, комплексом программных средств прикладной системы (КПСИС) и ЕС ИФЮЛ.

КП используется для работы непосредственно с ЕС ИФЮЛ и КПСИС для аутентификации владельца КТА или средства ЭЦП, подписи данных и организации защищенного соединения.

КПСИС предназначена для быстрой интеграции ПС с БИСРС, защиты передаваемых персональных данных, выработки/проверки ЭЦП и организации защищенного соединения.

Список литературы

1. Государственная программа развития цифровой экономики и информационного общества на 2016–2020 гг. : в ред. пост. Совета Министров Респ. Беларусь от 9 ноября 2018 г. № 806.

2. Поручение Совета Министров Республики Беларусь от 15.10.2018 № 33/216-298/11764р.

3. Разработка комплекса программно-аппаратного «Национальная инфраструктура открытых ключей для поддержания механизмов защиты данных, хранящихся в электронных машиносчитываемых проездных документах» : отчет об опытно-конструкторской работе.

4. Единая система идентификации физических и юридических лиц. Программное обеспечение. Пояснительная записка. БФИД.10243-01 81 01-ЛУ.

УДК 003.26+004.032.26

ИСКУССТВЕННЫЕ НЕЙРОННЫЕ СЕТИ В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ

М.В. МАЛЬЦЕВ
Научно-исследовательский институт прикладных проблем математики и информатики г. Минск, Республика Беларусь

Введение. Нейронные сети – активно развивающийся инструмент, доказавший свою эффективность для решения многих практических задач анализа данных. Нейронные сети применяются в задачах распознавания, классификации, анализа данных и прогнозирования, построения систем искусственного интеллекта. В последние годы интерес к нейронным сетям появился и в криптографическом сообществе. Ведутся исследования по применению нейронных сетей для анализа криптографических алгоритмов и протоколов, для разработки и анализа генераторов псевдослучайных чисел, обнаружения вторжений и для других задач. Одной из ключевых особенностей нейронных сетей является отсутствие необходимости четкого знания алгоритма для решения задачи – сеть в процессе обучения самостоятельно вырабатывает наиболее эффективный по заданным критериям алгоритм. Применению нейронных сетей в задачах защите информации посвящена настоящая статья.

1. Искусственные нейронные сети. Идея искусственных нейронных сетей состоит в моделировании работы человеческого мозга, состоящего из множества взаимодействующих между собой нервных клеток – нейронов. У типичного нейрона имеется несколько «входных» отростков – дендритов, через которые он получает сигналы от других нейронов, и один «выходной» отросток – аксон, по которому нейрон передает свой сигнал. Моделируя эту структуру, американский ученый Фрэнк Розенблатт в 1950-х годах предложил конструкцию перцептрона, являющуюся основой нейронных сетей. Схема перцептрона представлена на рисунке 1 [1].

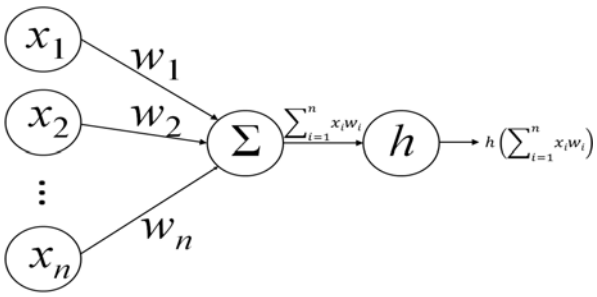


Рис. 1. Схема перцептрона

Здесь $x_1, x_2, ..., x_n$ – входные значения нейрона из некоторого множества (например, из множества действительных чисел □); $w_1, w_2, ..., w_n$ – веса входных значений. Основной задачей при работе с нейронной сетью является ее обучение – определение весов w_i. Функция h называется функцией активации. Распространенным на практике являются следующие типы функций:

– логический сигмоид:

$$h(\mathrm{z}) = \frac{1}{1+e^{-z}};$$

– гиперболический тангенс:

$$h(\mathrm{z}) = \frac{e^{z}-e^{-z}}{e^{z}+e^{-z}};$$

– функция Хевисайда:

$$h(\mathrm{z}) = \begin{cases} 0, \textit{если } z \le 0, \\ 1, \textit{если } z > 0. \end{cases};$$

– ReLU (rectified linear units):

$$h(\mathrm{z}) = \begin{cases} 0, \textit{если } z \le 0, \\ z, \textit{если } z > 0. \end{cases};$$

Множество соединенных друг с другом перцептронов (как правило, в слои), образуют нейронную сеть. Схема нейронной сети приведена на рисунке 2. В зависимости от строения (архитектуры) выделяют различные типы нейронных сетей: сверточные сети, рекуррентные сети, генеративно-состязательные нейронные сети и другие [1].

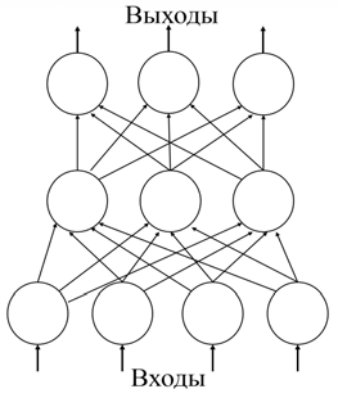


Рис. 2. Схема нейронной сети

2. Применение нейронных сетей в задачах информационной безопасности. Важной практической задачей, решаемой с помощью искусственных нейронных сетей, является классификация. В связи с этим значительное число публикаций посвящено применению нейронных сетей для построения систем идентификации и аутентификации, использующих биометрические характеристики: отпечатки пальцев, изображения лица, радужную оболочку глаза, почерк и др. [2–4]. В [4] сверточные нейронные сети применены для построения системы защиты криптовалютного кошелька: владелец кошелька идентифицируется по изображению его лица; точность распознавания, вычисленная в компьютерных экспериментах, составила 99.3%. Следует отметить, что для разработки методов распознавания пользователей информационных систем по их биометрическим характеристикам требуются достаточно большие базы таких характеристик, получить которые зачастую затруднительно. Решить указанную проблему помогают генеративно-состязательные нейронные сети, которые позволяют создавать необходимые данные. Такие сети, как правило, состоят из двух компонент – генератора и дискриминатора: генератор порождает объекты, принадлежащие различным классам, а дискриминатор пытается отличать объекты из разных классов – в результате такого взаимодействия качество объектов генератора улучшается. В работе [5] генеративно-состязательные нейронные сети применены для генерации отпечатков пальцев.

Применяются нейронные сети и для построения и анализа криптографических алгоритмов и протоколов. В работах [6, 7] нейронные сети используются для конструирования блочных и поточных шифров, в [8, 9] – для функций хэширования. В [9] нейронная сеть с одним скрытым слоем вычисляет 128-битное хэш-значение. Проведено исследование криптографических свойств построенной функции: стойкость к атаке нахождения прообраза, к атаке «дней рождения». Наличие лавинного эффекта проиллюстрировано на рисунке 3: по горизонтальной оси откладывался номер бита, изменяемого в сообщении, по вертикальной оси – расстояние Хэмминга между хэш-значениями исходного сообщения и измененного. Расстояние Хэмминга колеблется около 50, что говорит о наличии лавинного эффекта: изменение одного бита влечет изменение около половины бит хэш-значения. Предложенная в [9] хэш-функция допускает распараллеливание, что позволило добиться превосходства в скорости над хэш-функциями MD5 и SHA-1.

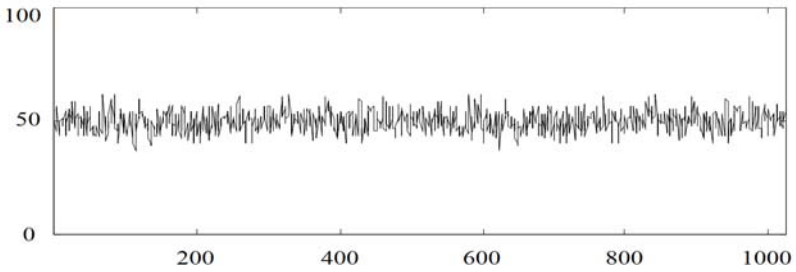


Рис. 3. Зависимость хэш-значения от изменения бит сообщения

Ряд публикаций посвящен применению нейронных сетей для криптоанализа систем шифрования [10–12]. Статья [11] посвящена атакам по сторонним каналам, использующим особенности практической реализации криптографических алгоритмов, которые могут приводить к уязвимостям. Анализируются показатели физических процессов, происходящих в конкретном устройстве, на котором реализован криптографический алгоритм: время выполнения алгоритма, потребляемая мощность, напряжение и сила тока в узлах устройства и другие характеристики. На основании этих данных становится возможным за сравнительное небольшое время извлекать информацию о секретных параметрах криптосистемы. В [11] применение сверточных нейронных сетей позволило повысить эффективность подобных атак.

В работе [12] нейронные сети применялись для распознавания шифртекстов различных криптосистем. Для этого использовались каскадные корреляционные нейронные сети (cascade correlation neural networks) и сети с обратным распространением ошибки (back propagation networks). Анализировались выходные последовательности блочного шифра RC6e (enhanced

RC6) и поточного шифра SEAL. В ходе вычислительных экспериментов использовался шифртекст длиной 1,92 миллиона символов, из которых 1,66 миллиона использовались для обучения нейронной сети, остальные 260 тысяч – для проверки качества распознавания. Нейронные сети позволили достичь высокой точности классификации: для сети с обратным распространением ошибок она составила 85%, для каскадной корреляционной сети – 92%.

В завершение приведем работу сотрудников компании Google [13], в которой исследовалась возможность построения нейронными сетями криптографических алгоритмов, обеспечивающих конфиденциальную передачу информации. Для этой цели использовались уже упоминаемые в настоящей статье генеративно-состязательные нейронные сети. Моделировались три сети: Алиса, Боб и Ева. Алиса и Боб, имеющие общий секретный ключ, обмениваются сообщениями по открытому каналу связи, прослушиваемому Евой. Цель Алисы и Боба состоит в обеспечении конфиденциальности их переписки, цель Евы – нарушить эту конфиденциальность. Отметим, что никакого априорного знания алгоритмов шифрования во взаимодействующие нейронные сети не закладывалось. В результате Алиса и Боб обучаются симметричному шифрованию, «изобретая» некоторое подобие одноразового блокнота. Результаты вычислительных экспериментов представлены на рисунке 4. Передаваемые секретные сообщения представляли собой случайные 16-битовые последовательности. Задача Боба и Евы состояла в восстановлении переданного Алисой сообщения. На рисунке 4 представлены графики зависимости ошибок Боба и Евы от числа итераций обучения. Видно, что со временем Боб обучается безошибочно расшифровывать сообщение, а Ева ошибается в восьми битах, что соответствует случайному угадыванию открытого текста.

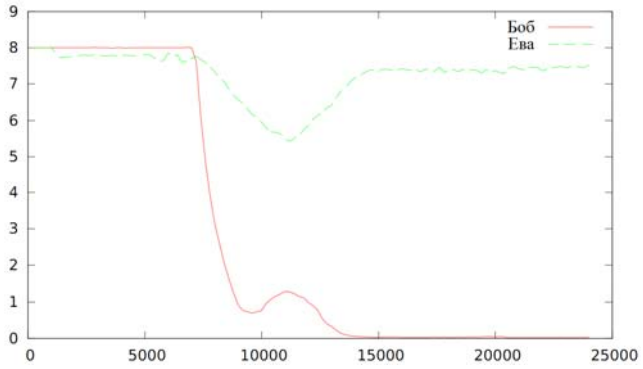


Рис. 4. Зависимость ошибок от числа итераций обучения

Список литературы

1. Николенко, С. Глубокое обучение / С. Николенко, А. Кадурин, Е. Архангельская. – СПб. : Питер, 2018. – 480 с.

2. Rathgeb, C. A survey on biometric cryptosystems and cancelable biometrics / C. Rathgeb, A. Uhl // EURASIP Journal on Info. Security. – 2011. – № 3.

3. Tarek, M. Robust cancellable biometrics scheme based on neural networks / M. Tarek, O. Ouda, T.Hamza // IET Biometrics. – 2016. – № 5 – P.220–228.

4. Albakri, A. Convolutional neural network biometric cryptosystem for the protection of the blockchain's private key / A. Albakri, C. Mokbel // Procedia Computer Science. – 2019. – Vol. 160. – P. 235–240.

5. Riazi, M. Automatic Synthetic Fingerprint Generation / M. Riazi, S. Chavoshian, F. Koushanfar . – 2020.

6. Long, H. Stream Cipher Method Based on Neural Network / H. Long // Proceedings of the 2012 National Conference on Information Technology and Computer Science, CITCS. – 2012. – P. 414–417.

7. Lian, S. A block cipher based on chaotic neural networks / S. Lian // Neurocomputing. – 2009. – Vol. 72. – P. 1296–1301.

8. Turcanik, M. Hash function generation by neural network / M. Turcanik, M. Javurek // New Trends in Signal Processing (NTSP). – 2016. – P. 1–5.

9. Lian, S. One-way Hash Function Based on Neural Network / S.Lian, J.Sun, Z. Wang. – 2007.

10. Xiao, Y. Neural Cryptanalysis: Metrics, Methodology, and Applications in CPS Ciphers / Y. Xiao, Q. Hao, D. Yao // 2019 IEEE Conference on Dependable and Secure Computing (DSC). – 2019. – P. 1–8.

11. Cagli, E. Convolutional neural networks with data augmentation against jitter-based countermeasures / E. Cagli, C. Dumas, E. Prouff // International Conference on Cryptographic Hardware and Embedded Systems. – 2017. – P. 45–68.

12. Chandra, B. Applications of cascade correlation neural networks for cipher system identification / B. Chandra, P. Varghese // World Academy of Science, Engineering and Technology, Vol. 26. P. 312–314, 2007.

13. Abadi, M. Learning to protect communications with adversarial neural cryptography / M. Abadi, D. G. Andersen. – 2016.

УДК 003.26.09

ИНТЕГРАЛЬНО-ЛИНЕЙНЫЙ КРИПТОАНАЛИЗ БЛОЧНЫХ ШИФРСИСТЕМ

Д.А. ФЕДЧЕНКО
Оперативно-аналитический Центр при Президенте Республики Беларусь
г.Минск, Республика Беларусь

Введение. Современные шифрсистемы разрабатываются с учетом необходимости обеспечения высокой устойчивости к интегральному и линейному методам криптоанализа. В связи с этим, данные методы зачастую оказываются эффективными лишь для уменьшенных версий шифров, и неприменимы к полнораундовым алгоритмам. В ходе исследования стойкости шифра Калина к интегральному и линейному методам [1] возникла идея метода, объединяющего обе эти техники. Данная работа посвящена описанию ключевых идей этого метода, и изучению возможностей его практического применения. Изложение метода производится в терминах работ [1] и [2].

1. Формулировка метода. Для применения интегрально-линейного метода алгоритм разбивается на три последовательные части: для первой части применяется некоторое интегральное соотношение для второй части строится согласованная система локальных линейных вероятностных соотношений специального вида, а в третьей части опробуются некоторые байты ключа.

Рассмотрим некоторый XSLP-алгоритм с длиной блока N_b байт, для которого атакующему известен r-раундовый интеграл, который имеет на выходе хотя бы один подблок удовлетворяющий свойству *S*. Это, в частности, означает, что при суммировании соответствующих подблоков промежуточных текстов из мультимножества $X^{(r)} = \{X^{(r)}_1, \ldots, X^{(r)}_N\}$ получаемого после *r* раундов алгоритма, получается нулевой знак (байт). Обозначим бит с номером *i* состояния $X^{(r)}_j$ символом $x^{(r)}_{j,i}$. Для удобства дальнейшего изложения идей метода будем считать, что свойство *S* выполняется для всех подблоков $X^{(r)}$. В таком случае, оказывается верным следующее соотношение:

$$\sum_{j=1}^{N} x^{(r)}_{j,i} = 0, \forall i \in \overline{0, N_b \cdot 8 - 1}.$$

Рассмотрим теперь систему локальных линейных вероятностных соотношений *L* для раундов *r*, … , *r* + 1, и пару вектор-столбцов (L'_L, L''_L), для которой выполняется условие ее согласованности, а двоичный вес вектора L'_L был равен единице. Будем считать, что единственный ненулевой бит данного вектора имеет номер $i \in \overline{0, N_b \cdot 8 - 1}$. Точное значение преобладания системы *L* обозначим символом δ_L.

Интегрально-линейный метод является методом криптоанализа по подобраному открытому тексту. Атакующий опробует раундовые ключи третьей части алгоритма шифрования, и с их помощью вычисляет по известным блокам шифрованного текста, промежуточные тексты. Впрочем, на самом деле, оказывается достаточным вычисления лишь бит $X^{(r+l)}_j$ с номерами, на которых расположены единицы в векторе L''_L. После чего, происходит «вычисление» бит $x^{(r)}_{j,i} = L''_L \cdot X^{(r+l)}_j$. При этом, вероятность выполнения соотношения $x^{(r)}_{j,i} = x^{(r)}_{j,i}$ равна $\frac{1+\delta_L}{2}$.

Рассмотрим сумму $S = \sum_{j=1}^{N} x^{(r)}_{j,i}$ в нескольких альтернативных ситуациях. Естественно предположить, что при расшифровании на ложном ключе, получаемые биты промежуточных шифрованных текстов на выходе *r*-го раунда распределены случайно и равновероятно. В таком случае, вероятность p_{rand} того, что выполняется соотношение $S = 0$, равна вероятно-

сти того, что в наборе бит промежуточных шифрованных текстов содержится четное количество единиц, то есть:

$$p_{rand} = \sum_{i=0}^{N/2-1} \frac{C_N^{2i}}{2^N} = \frac{1}{2^N} \cdot \sum_{i=0}^{N/2-1} C_N^{2i} = 2^{-N} \cdot 2^{255} = 0{,}5.$$

В случае же расшифрования на истинном ключе, вероятность p_{true} того, что вычисляемая сумма равна нулю, равна вероятности того, что соотношение $x_{j,i}^{(r)} = x_{j,i}^{(r)}$ не выполнилось четное число раз, то есть:

$$p_{rand} = \sum_{i=0}^{N/2-1} C_N^{2i} p^{2i} q^{N-2i}, \text{ где } p = \frac{1+\delta_L}{2}, q = \frac{1-\delta_L}{2}.$$

Теоретическая возможность статистической отбраковки ложных ключей следует из того факта, что для значений $\delta_L \in (0,1]$ верно неравенство $p_{true} > p_{rand}$. Пусть $\delta_{true} = 2p_{true} - 1$. Хтобы отбраковать все ложные ключи с вероятностью, близкой к единице, необходимо вычислить сумму S порядка $\frac{c}{\delta_{true}^2}$ раз для некоторого значения c. Таким образом, для эффективного, то есть с вероятностью отбраковки всех ложных ключей близкой к единице, применения интегрально-линейного метода требуется $T = N \cdot \frac{2}{\delta_{true}^2}$ подобранных пар открытого и шифрованного текста.

2. Применение интегрально-линейного метода. Величина δ_{true} зависит от двух параметров атаки: преобладания δ_L согласованной системы локальных линейных вероятностных соотношений для раундов $r - l$, а также от мощности N мультимножеств задействованных в интегральном соотношении. Максимизации δ_{true} можно достигнуть с помощью максимизации параметра δ_L, либо минимизации значения N.

Первый способ отсылает нас к основам линейного криптоанализа. В настоящее время имеется ряд подходов к повышению эффективности использования линейных соотношений. Одним из них являтся множественный линейный криптоанализ. Данный способ предполагает построение нескольких линейных соотношений для вычисления одного бита промежуточных данных. Совместный подсчет статистик для всех найденных соотношений позволяет получать большее количество информации о бите раундового ключа. Подробное описание метода и анализ его эффективности представлены в работах [4] и [5].

В то же время, задача минимизации значения N – количества блоков открытого текста, используемых в одном интегральном соотношении, не является столь активно изучаемой в открытой литературе. При исследовании стойкости алгоритма шифрования к интегральному методу, криптографами как правило ищутся интегралы, задействующие как можно большее количество раундовых преобразований. Польза от решения задачи по поиску интегралов малой мощности состоит не только в повышении эффективности использования интегрально-линейного криптоанализа, но и получении возможности строить менее трудоемкие и требовательные к материалу атаки интегральным методом.

В связи с этой задачей уместно упомянуть понятие разделительного свойства, впервые введенное в работе [3] в контексте построения интегральных соотношений для алгоритмов блочного шифрования. В отличие от классического интегрального метода, в котором не используются по существу, за исключением биективности, свойства S-боксов, разделительное свойство опирается на показатели алгебраической степени нелинейности. В случае S-боксов шифра Калина данные показатели достигают максимально возможного значения для подстановок такого размера, то есть 7.

Для краткости, под (l, d, m)-XSL алгоритмом будем понимать XSL алгоритм с m S-боксами длины l и алгебраической степенью нелинейности d. Отметим, что в смысле таких обозначений, шифры Калина, AES и Кузнечик аналогичны, так как все они являются (8, 7, 16)-XSL алгоритмами.

В таблице 1 приведены результаты работы алгоритма, сформулированного в работе [3]. Данный алгоритм позволяет вычислять оценки количества материала, необходимого для построения интегральных соотношений в зависимости от параметров (l, d, m)-XSL алгоритма.

Таблица 1

Объем необходимого материала для построения интегрального различителя

Алгоритм шифрования	Параметры			Объем материала				
	l	d	m	$r = 3$	$r = 4$	$r = 5$	$r = 6$	$r = 7$
Мини-Калина	4	3	16	2^{12}	2^{28}	2^{52}	2^{60}	–
Калина 128/256	8	7	16	2^{56}	2^{120}	–	–	–
AES	8	7	16	2^{56}	2^{120}	–	–	–
Serpent	4	3	32	2^{12}	2^{28}	2^{84}	2^{113}	2^{124}

Отсюда, в частности, следует невозможность эффективного применения интегрально-линейного метода к шифрам Калина и AES. Действительно, в работе [1] продемонстрировано, что построение интегральных различителей даже для трех раундов требует значительных объемов материала.

3. Анализ зависимостей параметров атаки. Интегрально-линейный метод существенным образом зависим от мощности используемого интеграла. В частности, для интегралов мощностью превышающей 2^8, значение δ_{true} оказывается слишком близко к δ_{rand} для эффективного применения интегрально-линейного метода.

На рисунке 1 продемонстрированы зависимости δ_{true} от δ_L при некоторых фиксированных мощностях интегральных соотношений: $N = 2^4$, $N = 2^6$ и $N = 2^8$.

Из них видно, что значение δ_{true} оказывается близким к нулю при $\delta_L < 0{,}75$ для мощностей N, превышающих 2^4. Отметим, что такие значения преобладания не позволяют строить эффективные атаки по причине чрезмерно высоких требований к объему подбираемого материала. В случае $N = 2^8$, характерного, например, для некоторых интегралов алгоритмов Калина и AES, значение δ_{true} оказывается близким к нулю при $\delta_L < 0{,}98$.

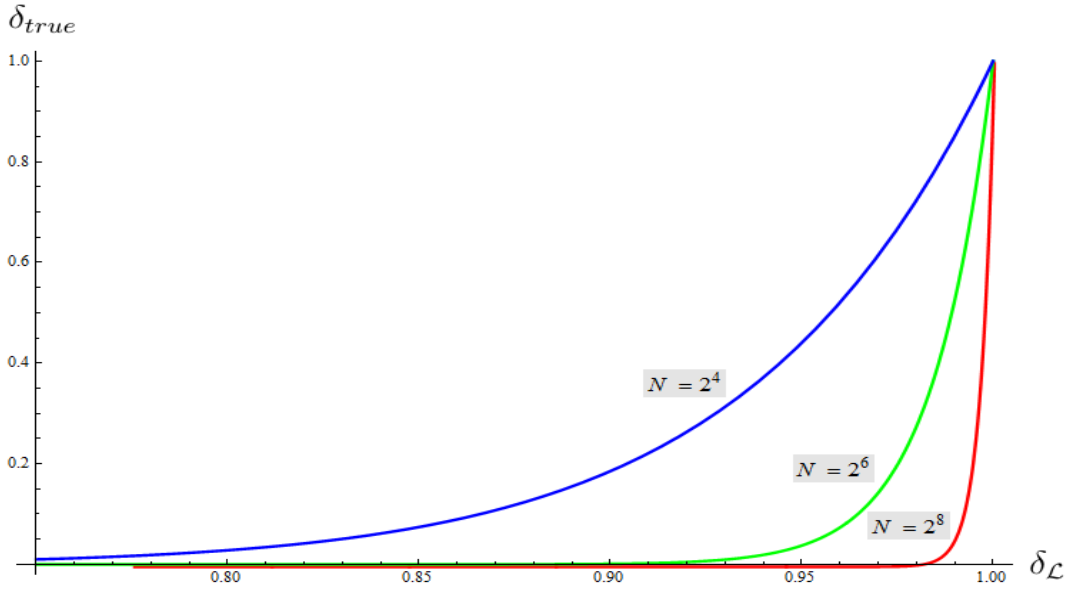


Рис. 1. Графики зависимости δ_{true} от δ_L при фиксированных мощностях интегральных соотношений $N = 2^4$ (синий), $N = 2^6$ (зеленый), $N = 2^8$ (красный)

Рисунки 2 и 3 призваны продемонстрировать зависимость δ_{true} от мощности используемого интегрального соотношения N при фиксированном преобладании согласованной системы локальных линейных вероятностных соотношений δ_L в интегрально-линейном методе.

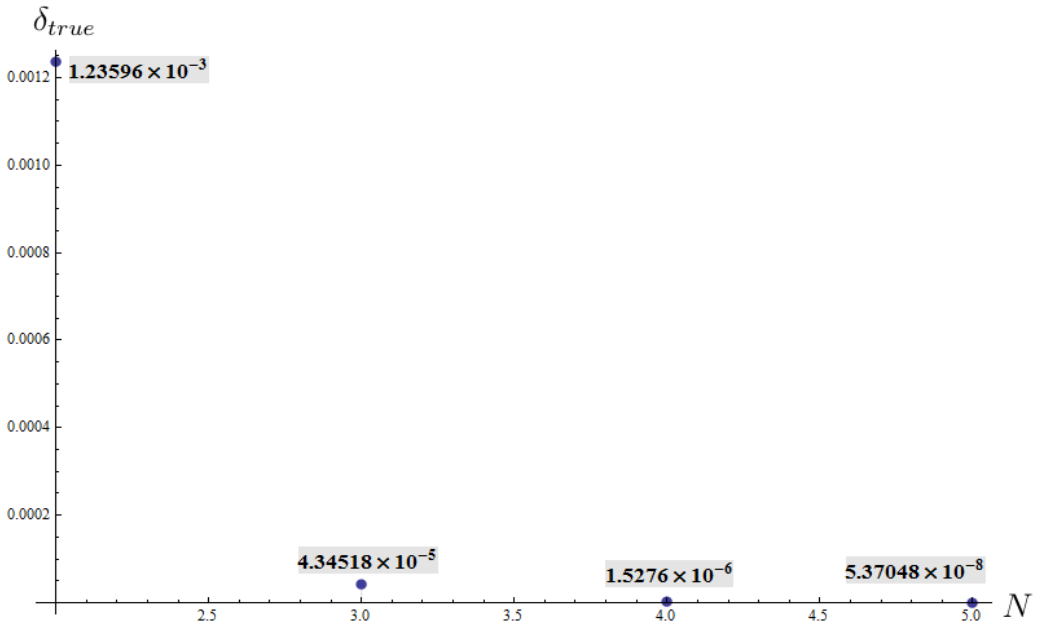


Рис. 2. График зависимости δ_{true} от N при фиксированном преобладании $\delta_L = 0{,}1875$

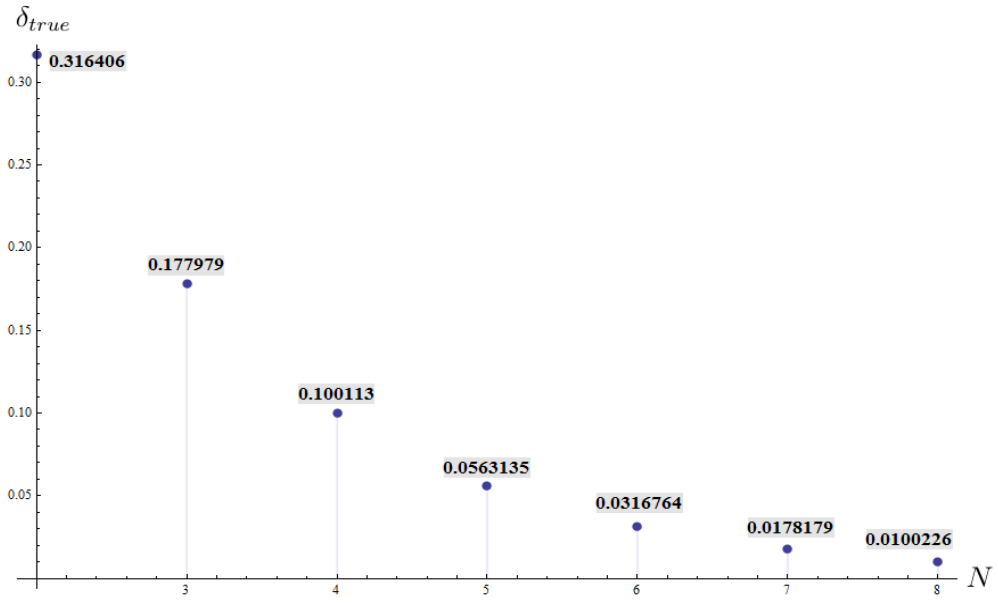


Рис. 3. График зависимости δ_{true} от N при фиксированном преобладании $\delta_L = 0{,}75$

Заключение. В условиях многообразия подходов к криптоанализу блочных шифров, существенный научный интерес представляет объединение различных подходов с целью увеличения количества раундов, подвергаемых атаке. Таким образом всякий прогресс в исследовании отдельных подходов, будет положительно сказываться на качестве «гибридных» атак, что, в конечном счете, может привести к новым результатам в области криптоанализа полнораундовых версий блочных шифров.

Список литературы

1. Федченко, Д. А. Анализ алгоритма Калина 128/256 с уменьшенным числом раундов интегральным методов / Д. А. Федченко // Теоретическая и прикладная криптография. – 2020.

2. Matsui, M. Linear cryptanalysis method for DES cipher / M. Matsui // EUROCRYPT. – 1993.

3. Todo, Y. Structural Evaluation by Generalized Integral Property / Y. Todo // EUROCRYPT. – 2015.

4. Kalinski, B. S. Linear Cryptanalysis Using Multiple Approximations / B. S. Kalinski Jr., M. J. B. Robshaw. – 1994.

5. Biryukov, A. On Multiple Linear Approximations / A. Biryukov, C. De Canniere, M. Quisquater – 2004.

УДК 004.056

АНАЛИЗ БЕЗОПАСНОСТИ ИСХОДНОГО КОДА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КАК ЭЛЕМЕНТ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

М.А. БАБИЧ
Министерство обороны Республики Беларусь, г. Минск, Республика Беларусь

В настоящее время в Республике Беларусь самой динамично развивающейся отраслью является индустрия информационных технологий. Резкое повышение спроса на разработку программного обеспечения, которое наблюдается в последние годы, не удовлетворяется кадровыми предложениями рынка. Как следствие, Республика Беларусь как и весь развитый мир испытывает нехватку в опытных программистах. Вместе с тем, при разработке программного кода его тестированию по требованиям информационной безопасности не уделяется должного внимания. Несмотря на совершенствование инструментов разработки, создание новых подходов к проектированию и программированию, непрерывно растет сложность задач, и как следствие – написанного кода. Это в свою очередь ведет к увеличению риска появления критических ошибок и уязвимостей.

Анализ кода по требованиям информационной безопасности – не менее важный этап разработки, чем комплексное тестирование в рамках проведения опытной эксплуатации. Он позволяет выявлять уязвимости информационной безопасности, умышленно или неумышленно допущенные при разработке. Особенно это актуально для критически важных объектов инфраструктуры, автоматизированных систем управления и образцов вооружения.

В настоящее время в Вооруженных Силах Республика Беларусь в основном применяются следующие методы анализа безопасности исходного кода:

– динамический метод – метод анализа безопасности программного обеспечения, требующий выполнения программ на специальном стенде, с доступом к исходному коду и среде его функционирования;

– статический метод – метод анализа безопасности программного обеспечения с доступом к исходному коду и не требующий выполнения программ;

– гибридный метод – метод, совмещающий два предыдущих метода.

Реже применяется метод ручной инспекции кода (code review), фаззинг-тестирование **и** другие. Дополнительными мерами, применяемыми для анализа и повышения уровня информационной безопасности, можно считать использование:

- систем управления версиями и ветками релизов (SVN и Git);
- систем отслеживания ошибок (bug tracking system);
- систем непрерывной интеграции и непрерывного развертывания (CI/CD).

Для повышения уровня безопасности кода используются следующие общие требования:

1. Проверка всех входных и выходных данных.
2. Запрет на предоставление пользователю избыточных данных.
3. Максимально допустимое ограничение прав пользователя.
4. Ведение журналов безопасности и действий пользователей.
5. Ограничение действий пользователей по принятию не регламентированных решений.
6. Контроль кода на избыточность.
7. Контроль версий, квот и буферов.
8. Использование стандартных средств операционной системы.
9. Безопасное создание и удаление временных файлов и переменных.
10. Запрет на использование внутрикорпоративных названий.

Кроме того, выработаны общие рекомендации безопасного написания кода для разработчиков:

1. Использовать стили программирования и стандарты безопасного написания для конкретного языка.

2. Минимизировать использование внешнего кода от сомнительных или неизвестных источников.

3. Учитывать предупреждения компилятора.

4. Проектировать с возможностью разделения привилегий.

5. Придерживаться простоты в проектировании и разработке.

6. Создавать предсказуемые конструкции, обладающие гибкостью и масштабируемостью (концепция SOLID).

7. По умолчанию запрещать и использовать наименьшие из возможных привилегий.

8. Исключать лишнюю информацию при взаимодействии с внешними системами.

9. Организовывать защиту на всех уровнях.

10. Использовать системы контроля качества кода, системы управления версиями и ветками релизов, системы отслеживания и управления ошибками, системы непрерывной интеграции и непрерывного развертывания.

В большинстве случаев анализ защищенности программного обеспечения включает в себя следующие стадии:

1. Анализ защищенности методами «черного» и «серого ящика», т. е. динамический анализ безопасности программного обеспечения без доступа к исходному коду:

- метод «черного ящика» направлен на поиск уязвимостей, использование которых позволяет не имеющему никаких привилегий злоумышленнику реализовать следующие виды угроз: получение несанкционированного доступа к информации, полный или частичный контроль над приложением и его использование для организации атак;

- метод «серого ящика» аналогичен предыдущему, с тем лишь исключением, что под злоумышленником подразумевается пользователь, обладающий определенным набором привилегий.

2. Анализ защищенности методом «белого ящика» – динамический и статический анализ безопасности исходного кода. Выполняется анализ исходного кода с помощью специализированного программного обеспечения (анализаторы исходного кода), позволяющего фиксировать подозрения на уязвимости. Для разных языков и платформ используются различные анализаторы.

На этом этапе особое внимание уделяется следующим «чувствительным местам» в коде:

- механизмам валидации и нормализации вводимых данных;

- механизмам аутентификации и авторизации;

- механизмам криптозащиты;

- механизмам защиты хранимых данных на предмет предотвращения несанкционированного доступа;

- протоколам обмена данными между клиентскими и серверными частями программного обеспечения.

3. Разработка рекомендаций и итогового отчета.

Перечень актуальных уязвимостей строится на основе отчетов работы специального программного обеспечения и журналов работы специальных стендов (песочниц), материалов свободных исследовательских групп по поиску уязвимостей, каталогов уязвимостей, в частности:

- Computer Emergency Readiness Team (CERT);

- Common Vulnerabilities and Exposures (CVE);

- Web Application Security Consortium (WASC);

- Open Web Application Security Project (OWASP);

- Open Source Vulnerabilities Database (OSVDB).

Для каждой уязвимости описываются возможные последствия ее эксплуатации. Вырабатываются предложения по устранению уязвимостей, выявленных в ходе анализа защищенности, или снижению ущерба от их реализации.

4. Проверка корректности устранения выявленных уязвимостей. Проводится проверка наличия выявленных уязвимостей и оценка эффективности принятых мер по их нейтрализации. Подготавливается отчет о проверке корректности устранения выявленных уязвимостей.

Комплексный подход, создание ведомственного подразделения разработчиков, использование современных методов и «лучших практик» программирования, анализ программного обеспечения на отсутствие недекларированных возможностей позволяет минимизировать угрозы информационной безопасности в корпоративном программном обеспечении.

В прошлом году в Вооруженных Силах Республики Беларусь проведены 19 проверок программного обеспечения, применяемого в ведомственных информационных системах и сетях.

Таким образом, в настоящее время в Вооруженных Силах Республики Беларусь создана и успешно функционирует система информационной безопасности, представляющая собой комплекс правовых, организационных и технических мер. Одним из элементов которой является анализ безопасности исходного кода программного обеспечения на наличие недекларированных возможностей и программных закладок.

УДК 004.056

ПРИМЕНЕНИЕ ТЕСТОВ НА ОСНОВЕ ЗАКОНА ПОВТОРНОГО ЛОГАРИФМА ДЛЯ ОЦЕНКИ КАЧЕСТВА СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

А.И. ТРУБЕЙ, В.Ю. ПАЛУХА, И.К. ПИРШТУК, А.А. ОРЛОВ
Учреждение БГУ «НИИ прикладных проблем математики и информатики»
г. Минск, Республика Беларусь

Введение. Существующие батареи статистического тестирования не охватывают некоторые основополагающие законы случайности. Существуют две фундаментальные предельные теоремы о случайных двоичных последовательностях – это центральная предельная теорема и закон повторного логарифма (ЗПЛ). Несколько тестов в батарее NIST SP800-22 включают центральную предельную теорему, в то время как ни один тест в батарее не охватывает закон повторного логарифма.

В докладе описывается методика принятия решений о качестве последовательностей с применением закона повторного логарифма, в которой в качестве статистического расстояния применяется статистика хи-квадрат согласия. Представлены результаты экспериментов по тестированию генераторов псевдослучайных последовательностей, в том числе последовательностей, сгенерированных линейным конгруэнтным генератором, а также разработанным сотрудниками НИИ ППМИ стандартом СТБ 34.101.47-2012 (в режиме счетчика). Идея тестирования с применением закона повторного логарифма (ЗПЛ-тестирования) была впервые предложена в статье [1] и развита в статье [2]. В работе [3] приведена двухэтапная процедура проверки гипотез с применением закона повторного логарифма для частного случая теста многомерной дискретной равномерности по непересекающимся отрезкам (при $L = 1$) – теста Монобит.

1 Тест многомерной дискретной равномерности по непересекающимся отрезкам. Тест многомерной дискретной равномерности по непересекающимся отрезкам (МДРН-тест) является одним из классических тестов, предложенных Кнутом. МДРН-тест предназначен для проверки гипотезы H_0 согласия наблюдаемой последовательности L-векторов с L-мерным дискретным равномерным распределением.

Пусть имеется двоичная последовательность:

$$X = \{x_1, x_2, ..., x_n\}$$

Разбиваем последовательность X на непересекающиеся отрезки длиной L:

$X_t = \{x_{L(t-1)+1}, ..., x_{Lt}\}, 1 \le t \le k$, где $k = \left[n / L \right]$ – число отрезков разбиения.

Проверку гипотез с применением закона повторного логарифма для МДРН-теста будем осуществлять в зависимости от длины L (на основании аппроксимации нормальным распределением схемы независимых испытаний Бернулли и распределения хи-квадрат).

1.1. Аппроксимация нормальным распределением схемы независимых испытаний Бернулли. При $1 \le L < L_0$ по наблюдаемой последовательности X_t строим 2^L вспомогательных двоичных последовательностей:

$$Y_v = \{y_1^{(v)}, ..., y_t^{(v)}, ..., y_k^{(v)}\}, 1 \le t \le k, \text{ где:}$$

$$y_t^{(v)} = 1, \text{ если } X_t = v; v \in \{0,1\}^L;$$

$$y_t^{(v)} = 0, \text{ если } X_t \ne v; v \in \{0,1\}^L.$$

Таким образом мы получим схему независимых испытаний Бернулли, где $p = 1/2^L$ – вероятность положительного исхода в одном испытании, $1 - p$ – вероятность отрицательного исхода. Вычислим 2^L статистик теста: $S_v(k) = \sum_{t=1}^{k} y_t^{(v)}$ (далее индекс v для удобства опустим).

Математическое ожидание и дисперсия статистики имеют следующий вид:

$$E\{S(k)\} = kp = \frac{k}{2^L};\ D\{S(k)\} = kp(1-p) = \frac{k}{2^L}\left(1-\frac{1}{2^L}\right).$$

Тогда при $k \to \infty$ статистика

$$S(k)^* = \frac{S(k)-kp}{\sqrt{kp(1-p)}} = \frac{\left\{S(k)-\frac{k}{2^L}\right\}}{\sqrt{\frac{k}{2^L}\left(1-\frac{1}{2^L}\right)}} \quad (1)$$

распределена асимптотически нормально по закону $N(0,1)$.

Согласно закону повторного логарифма (в общем виде) справедлива формула [3]:

$$\limsup_{k\to\infty} \frac{S(k)^*}{\sqrt{2\ln\ln k}} = \limsup_{k\to\infty} \frac{\frac{S(k)-kp}{\sqrt{kp(1-p)}}}{\sqrt{2\ln\ln k}} = 1. \quad (2)$$

В соответствии с вышеизложенным, для МДРН-теста при проверке гипотез с применением закона повторного логарифма будем использовать статистики:

$$S_{зпл}(k) = \frac{S(k)^*}{\sqrt{2\ln\ln k}} = \frac{\frac{S(k)-kp}{\sqrt{kp(1-p)}}}{\sqrt{2\ln\ln k}} = \frac{\frac{\left\{S(k)-\frac{k}{2^L}\right\}}{\sqrt{\frac{k}{2^L}\left(1-\frac{1}{2^L}\right)}}}{\sqrt{2\ln\ln k}}. \quad (3)$$

Нетрудно заметить, что при $L = 1$ формула (3) превращается в формулу для теста Монобит:

$$S_{зпл}(n) = \frac{S(n)^*}{\sqrt{2\ln\ln n}} = \frac{2S(n)-n}{\sqrt{2n\ln n\ln n}}. \quad (4)$$

Для МДРН-теста меру μ_k^U можно рассчитать следующим образом:

$$\mu_k^U\{(-\infty, z]\} = \Phi\left(z\sqrt{2\ln\ln k}\right) = \sqrt{2\ln\ln k}\int_{-\infty}^{z}\phi\left(s\sqrt{2\ln\ln k}\right)ds. \quad (5)$$

Таким образом, чтобы оценить качество генератора G с применением закона повторного логарифма для МДРН-теста при $1 \le L < L_0$, необходимо:

1. Осуществить генерацию набора $\mathrm{R} \in \Sigma^n$ из $m = 10000$ последовательностей возможно большей длины.

2. Разбить последовательности на непересекающиеся отрезки длиной L.

3. На первом этапе двухэтапной процедуры проверки гипотез вычислить значения статистики $S_{зпл}(k)$ по всем m последовательностям.

4. На втором этапе сравнить между собой вероятностные меры $\mu_k^{\mathrm{R}_k}$ и μ_k^U. Для сравнения будем использовать следующую статистику χ^2 согласия [3]:

$$\chi^2\left(v \in \{0,1\}^L\right) = \sum_{j=1}^{|B|}\frac{\left[v_k^{\mathrm{R}_k}(I_j) - mp_k^{\mathrm{U}}(I_j)\right]^2}{mp_k^{\mathrm{U}}(I_j)}, \quad (6)$$

где $v_k^{\mathrm{R}_k}(I_j)$ – частоты попадания значений статистики $S_{зпл}(k)$ в интервал I_j по всем m последовательностям; $p_k^{\mathrm{U}}(I_j)$ – теоретические вероятности попадания $S_{зпл}(k)$ в интервал I_j.

Полагаем, что генератор G прошел тестирование по МДРН-тесту с применением ЗПЛ, если P-значения статистик $\chi^2\left(v \in \{0,1\}^L\right)$ согласия для всех $v \in \{0,1\}^L$ превышают заданный уровень значимости α, то есть, $P_v \ge \alpha$.

1.2. Аппроксимация нормальным распределением распределения хи-квадрат. При длинах $L \geq L_0$ процесс принятия решения можно оптимизировать и вместо 2^L статистик использовать только одну статистику. С этой целью для $v \in \{0,1\}^L$ вычисляем частоты встречаемости по всем отрезкам:

$$\nu_v^L = \sum_{t=1}^{k} I\left\{ X_t^L = v \right\} \; v \in \{0,1\}^L .$$

Вычисляем статистику:

$$S(k) = \chi_l^2(k) = \sum_{v \in \{0,1\}^L} \frac{\left(\nu_v^L - \frac{k}{2^L} \right)^2}{\frac{k}{2^L}}, \text{ где } l = 2^L - 1 . \quad (7)$$

В силу центральной предельной теоремы, при большом числе степеней свободы распределение случайной величины $S(k) = \chi_l^2(k)$ может быть аппроксимировано нормальным распределением. Более точно, при $l \to \infty$:

$$\mathrm{L}\left\{ S(k)^* \right\} \to \mathrm{N}\,(0,1), \text{где } S(k)^* = \frac{S(k) - l}{\sqrt{2l}} . \quad (8)$$

При этом следует учитывать, что график плотности распределения хи-квадрат, в отличие от биномиального распределения, не является симметричным. Математическое ожидание больше моды этого распределения, потому что правый хвост «тяжелее» левого. Поэтому полученный в результате нормировки график плотности распределения хи-квадрат (8) также не будет симметричным. Однако с увеличением числа степеней свободы графики становятся все более симметричными, то есть значения моды и математического ожидания постепенно сближаются. Необходимо экспериментально определить длину отрезка L_0, для которого при $L \geq L_0$ это будет давать аппроксимацию, достаточную для практических целей.

В таблице 1 приведены значения математических ожиданий M статистики хи-квадрат и их p-значений в зависимости от длин отрезков L.

Таблица 1

Зависимость *p*-значений математических ожиданий статистики хи-квадрат от длин отрезков *L*

Длина отрезка L	5	6	7	8	9	10	11	12
$M = 2^L - 1$	31	63	127	255	511	1023	2047	4095
p-значения	0,4662	0,4763	0,4833	0,4882	0,4916	0,4941	0,4958	0,4971

На рисунке 1 приведены графики плотности распределения хи-квадрат для различного числа степеней свободы.

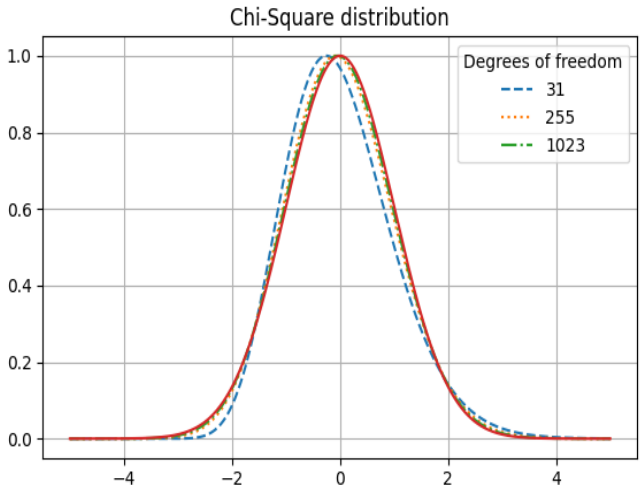


Рис. 1. Графики плотности нормированного распределения хи-квадрат для L = 5, 8, 10, 12

Из таблицы 1 и рисунка 1 видно, что уже при $L \geq 10$ левый и правый «хвосты» распределения хи-квадрат становятся практически симметричными.

Следовательно, для МДРН-теста при $L \geq 10$ можно использовать статистику:

$$S_{зпл}(k) = \frac{S(k)^*}{\sqrt{2\ln\ln k}} = \frac{\frac{S(k)-l}{\sqrt{2l}}}{\sqrt{2\ln\ln k}} = \frac{\frac{\left\{S(k)-\left(2^L-1\right)\right\}}{\sqrt{2\left(2^L-1\right)}}}{\sqrt{2\ln\ln k}}. \quad (9)$$

Полагаем, что генератор G прошел тестирование по МДРН-тесту с применением закона повторного логарифма, если P-значение статистики χ^2 согласия превышает заданный уровень значимости α, то есть, $P_v \geq \alpha$.

2. Экспериментальные результаты. Для проверки гипотезы проведено тестирование 10 000 последовательностей, выработанных соответственно линейным конгруэнтным генератором (ЛКГ) и стандартом СТБ 34.101.47-2012 (в режиме счетчика).

ЛКГ определяется рекуррентным соотношением $X_{n+1} = aX_n + c\left(\mathrm{mod} m\right)$, где X_n – последовательность псевдослучайных чисел, m – модуль, $a, c < m$.

Для любого начального значения X_0 последовательность имеет вид $X_0, X_1, \ldots, X_i, \ldots$ где X_i – двоичное представление целого числа X_i.

Результаты сравнительного тестирования по МДРН-тесту с применением закона повторного логарифма приведены в таблице 2.

Таблица 2

Результаты тестирования по МДРН-тесту последовательностей, выработанных ЛКГ и СТБ 34.101.47-2012 (в режиме счетчика), при L = 12

Объем, GB	ЛКГ			СТБ 34.101.47-2012		
	Степ. своб.	χ^2	P-знач.	Степ. своб.	χ^2	P-знач.
5	41	57.55	0.0446	41	27.30	0.9503
10	41	139.95	$9.8*10^{-13}$	41	45,25	0.2991

Из таблицы 2 видно, что для последовательностей (объемом 5 и 10 GB), сгенерированных в соответствии с СТБ 34.101.47-2012 (в режиме счетчика), выполняется гипотеза H_0 согласия с моделью независимых симметричных испытаний Бернулли на уровне значимости $\alpha = 0.05$. В то время как для последовательности, вырабатываемой линейным конгруэнтным генератором, гипотеза H_0 на данном уровне значимости не выполняется.

Гистограммы частот выборок, полученных с применением ЗПЛ по МДРН-тесту для линейного конгруэнтного генератора и алгоритма генерации псевдослучайных последовательностей в соответствии с СТБ 34.101.47-2012, приведены на рисунках 2, 3.

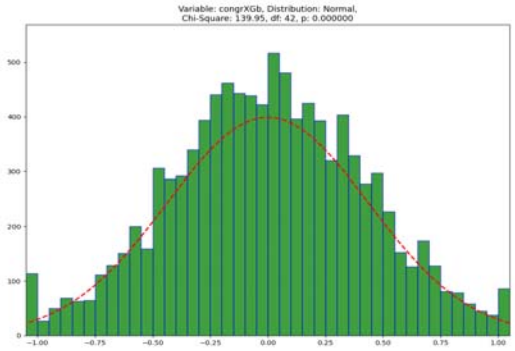


Рис. 2. Гистограмма частот линейного конгруэнтного генератора, 10 GB

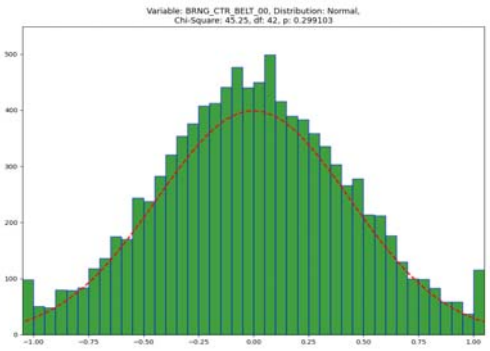


Рис. 3. Гистограмма частот алгоритма СТБ 34.101.47-2012, 10 GB

Список литературы

1. Wang, Y. Linear complexity versus pseudorandomness: on Beth and Dai's result / Y. Wang // Proc. Asiacrypt. – 1999. – P. 288–298.

2. Wang, Y. On statistical distance based testing of pseudorandom sequences and experiments with PHP and Debian OpenSSL / Y. Wang, T. Nicol // Computers & Security. 2015. – Vol. 53. – P. 44–64.

3. Трубей, А. И. Методика тестирования случайных последовательностей на основе статистического расстояния и закона повторного логарифма / А. И.Трубей [и др.] // Проблемы защиты информации : сб. науч. статей.

УДК 004.056

КЛЕПТОГРАФИЯ: МЕТОДЫ СИНТЕЗА И АНАЛИЗА КАНАЛОВ СКРЫТОЙ ПЕРЕДАЧИ ДАННЫХ

А.И. ТРУБЕЙ, М.Е. ШЕЛЕСТ
Учреждение БГУ «НИИ прикладных проблем математики и информатики»
г. Минск, Республика Беларусь

Введение. Окружающая нас информационная среда включает разнообразные программно-аппаратные средства для решения задач информационной безопасности, в том числе программно и аппаратно реализованные криптографические алгоритмы, которые для пользователей зачастую представляются как черные ящики. Конкретную структуру алгоритма сложно отследить даже в программных продуктах при отсутствии текстов исходных программ. И даже в тех случаях, когда спецификация становится доступной для пользователя, последний весьма редко проверяет соответствие имеющегося в его распоряжении продукта официальной документации. Таким образом, пользователи зачастую получают лишь иллюзию защиты. Используя алгоритм, все детали работы которого известны только его разработчику, пользователь располагает единственной гарантией стойкости – утверждением самого разработчика о надежности алгоритма. В то же время разработчики готовых продуктов объективно имеют возможность встроить лазейки в реализуемые криптографические алгоритмы по своей ли инициативе, по чьему-либо заказу или по указанию «сверху» [1].

Любое государство пытается контролировать, по крайней мере, свой сегмент киберпространства. Это возможно разными способами. Например, существует видимая коллаборация с государственными структурами (в первую очередь спецслужб США, Китая и России) крупных фирм-производителей микроэлектроники, вычислительной и телекоммуникационной техники с целью сбора информации о пользователях и доступе к их информации. В СМИ неоднократно появлялись данные о сотрудничестве со спецслужбами известных производителей средств телекоммуникаций (Cisco, Huaway), шифраторов (Crypto AG, Omnisec, Mils Electronic), программного обеспечения (Microsoft), социальных сетей (Facebook, Вконтакте, Одноклассники), антивирусных систем (Касперский, Radware, McAfee), поставщиков услуг электронной почты и сетевых Интернет-гигантов (Google, Yahoo, AT&T, CenturyLink, Verizon). Такое сотрудничество включает разработку и встраивание необходимых «бэкдоров» с последующей передачей спецслужбам тайных сведений о уязвимостях в аппаратном и программном обеспечении, в том числе и о действующих ключах шифрования [2].

1. Клептография и ее связь с криптографией и стеганографией. Вопросами разработки и встраивания закладок в системы защиты информации занимается клептография. Клептография изучает методы синтеза и анализа каналов скрытой передачи данных (embedded trapdoor, subliminal channel), которые позволяют лицу, внедрившего такой канал, получать чувствительную информацию относительно криптосистемы, ключей шифрования или организовывать извлечение защищаемых данных из информационных систем. Клептография стала системно развиваться в 70-х годах прошлого столетия с формированием рынка электронных шифраторов, а затем и открытого программного обеспечения, включая операционные системы. Методы клептографии в последнее время также успешно осваиваются и применяются хакерами.

Клептография, как направление информационной безопасности, тесно связана с криптографией и стеганографией (см. рисунок 1). Связь клептографии с криптографией обусловлена тем, что объектом ее исследований является клептографическая закладка (механизм), которая является частью криптосистемы. Методы криптоанализа часто используются для выявления закладок, то есть являются и инструментами клептоанализа. Клептография близка также к стеганографии. Общей отправной точкой как клептографии, так и стеганографии можно считать работы Г.Саймонса, в которых сформулированы и исследованы «проблема узника» («the prisoner’s problem») и скрытые каналы передачи («subliminal channels») [3, 4].

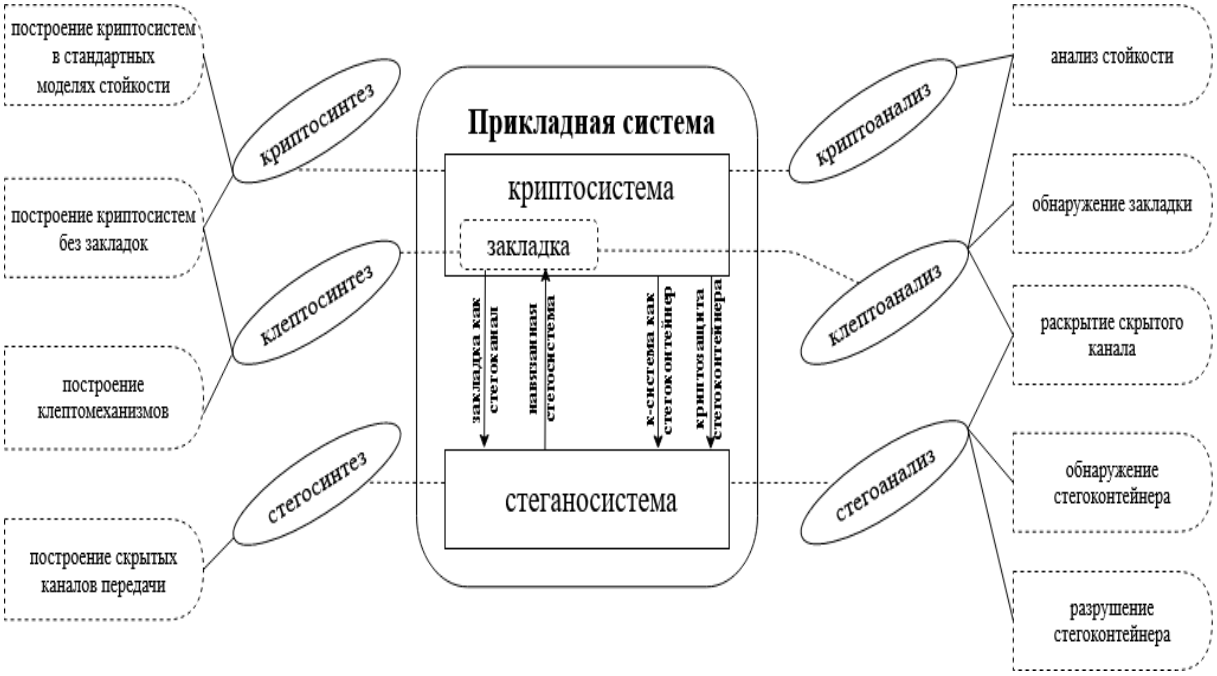


Рис. 1. Связь криптографии, стеганографии и клептографии

Криптоалгоритм с лазейкой (Backdoor, Trapdoor) – это алгоритм, который содержит некоторую скрытую структуру (лазейку), обеспечивающую существование скрытого канала передачи информации; знание этой структуры позволяет получать конфиденциальную информацию (например, о секретном ключе). Без знания лазейки алгоритм кажется надежным. Функционирование клептографических и стеганографических механизмов в некоторых аспектах схожи или пересекаются:

1.1. Клептомеханизм, который выполняет передачу секрета, может рассматриваться как стеганографический канал.

1.2. Скрытно встроенный стеганографический механизм может использоваться разработчиком для клептографических атак передачи секрета.

1.3. Клептографический механизм и стегосистема могут сосуществовать независимо. Например, в одной из модификаций SETUP, кроме схемы передачи ключа, существуют также стегоканалы, которые базируются на временных задержках отправления, вероятностном контроле определенных бит открытых случайных параметров, имитации сбоев и пр.

2. Основные направления развития клептографии. На данный момент, основным направлением практической клептографии является синтез криптосистем и криптопримитивов с соответствующими закладками. Криптосистемой с клептозакладкой будем называть такую криптосистему, у которой:

2.1. Структура системы сгенерирована с использованием «секрета разработчика».

2.2 «Секрет разработчика» практически невозможно получить путем анализа криптосистемы или такой анализ вообще невозможен.

2.3. Криптографические свойства системы существенно снижаются в случае знания «секрета разработчика».

То есть, в клептографической модели криптосистемы добавляется роль «разработчика», цель которого состоит в модифицировании (построении) криптосистемы таким образом, чтобы она содержала закладку, которая бы позволяла в процессе работы системы незаметно передавать определенную секретную информацию разработчику или упрощала ему задачу понижения криптографических свойств системы.

Построение канала утечки путем модификации реализации стандартного протокола – одна из наиболее изученных клептографических проблем [5]. Первой попыткой формализации клептографического механизма является модель SETUP (Secretly Embedded Trapdoor with Universal Protection), предложенная Яном и Юнгом, которая позволяет организовать скрытую передачу секретного ключа криптосистем на базе RSA и задачи дискретного логарифма [6].

Учитывая широкое использование криптографической защиты в информационно-телекоммуникационных системах, особую остроту приобретают вопросы защиты самих криптосистем на всех уровнях их жизненного цикла: этапе проектирования, реализации, развертывания и использования. Актуальными в этом аспекте являются вопросы:

– возможности построения криптосистем, устойчивых к различным типам клептографических атак;

– разработки критериев наличия/отсутствия клептографических закладок;

– синтеза криптографических систем и криптопримитивов с закладками с целью расширения множества шаблонов проектирования закладок для исследования методов их выявления и противодействия им.

Клептографические механизмы разнятся по сценарию построения, способу защиты канала разработчика, уровню абстракции и тому подобное. Известные работы, касающиеся проблем клептографии, фокусируются на отдельных алгоритмах с потенциальной закладкой или построением конкретных протоколов с каналами незаметной утечки секрета, поэтому разнообразие методов в определенной мере размывает общую картину направления. Классификация клептографических механизмов приведена в таблице 1.

Проблемой всех практических клептографических механизмов является то, что даже при нахождении закладки или канала утечки невозможно практически доказать «умышленность» ее построения, поскольку они также могут свидетельствовать лишь о недостаточности имеющихся методов или квалификации аналитиков. Поэтому под криптопримитивом с встроенным клептографическим механизмом мы понимаем такую схему, где только потенциально может быть намеренно организован канал утечки.

Таблица 1

Классификация клептографических механизмов

Тип классификации	Тип клептомеханизма	Примеры
По степени закрытости реализации	Закрытые стандартизованные реализации	Программные библиотеки, схемотехнические описания, спецификации алгоритмов
	Закрытые реализации	Проприетарные программные продукты с обфускацией программного обеспечения и потоков данных
	Аппаратные реализации	Криптографические микроконтроллеры, аппаратные криптомодули
По результатам анализа	Недеструктивные (с возможностью дальнейшего использования)	Анализ программных компонентов, маскирующихся аппаратных компонентов, логический анализ спецификаций и т. д.
	Деструктивные (без возможности дальнейшего использования)	Анализ криптографических контролеров, встроенной EEPROM-памяти и т. д.
По уровню построения	Модификация готовых криптосистем	Добавления канала утечки в реализацию системы, например, атака BEAST протокола TLS1.0 и ниже
	Построение новых криптоалгоритмов со встроенными закладками	Примеры вероятно таких алгоритмов: DES, DualEC, DRGB
По способу внедрения	Открытое распространение клептографических модификаций реализации алгоритмов	Например, в виде программных компонентов
	Распространения проприетарных закрытых криптосистем в виде аппаратных модулей	
	Лоббирование стандартизации клептографических криптосистем, навязывание их использования через правовые механизмы, корпоративные политики или маркетинговые кампании	

3. Краткий обзор современных клептографических механизмов. Приведем несколько примеров, которые, по всей вероятности, содержат клептографические механизмы:

3.1. Алгоритм шифрования DES. Алгоритм симметричного шифрования DES был предложен в 1974 году фирмой IBM, базируется на сети Фейстеля, размер открытого текста и сообщения составляет 64 бит, размер ключа – 56 бит. В оригинальную схему АНБ США был внесен ряд изменений (уменьшение длины ключа с 64 до 56 бит, «помощь» сотрудников АНБ в генерации *S*-блоков), что снизило устойчивость алгоритма к атакам перебора и дифференциальных анализа. Это наводило на подозрения, что такие изменения были внесены преднамеренно для того, чтобы спецслужбы США, имевшие достаточные вычислительные возможности, могли проводить дешифрование сообщений без знания секретных ключей. В частности, есть подозрения, что они владели методами дифференциального криптоанализа до его публикации Бихамом [7].

3.2 Система аппаратного шифрования Skipjack и стандарт EES. Стандарт EES (Escrowed Encryption Standard) аппаратного шифрования разработан АНБ США в рамках проекта Capstone для систем защищенной правительственной связи с закладкой. Стандарт включает в себя блочный алгоритм симметричного шифрования Skipjack и архитектуру LEAF (Law Enforcement Access Field – поле доступа для правоохранительных органов). Для имплементации стандарта использовался защищенный чип Clipper. Предполагалось, что стойкость шифратора будет базироваться на секретном алгоритме шифрования Skipjack, а процесс инициализации ключей будет производиться непосредственно разработчиком чипа. Архитектура LEAF позволяет использовать два ключа расшифрования: один – для пользователя, а другой – для правоохранительных органов. Поэтому разработчики могут расшифровывать перехваченное сообщение, в то время как обычные пользователи могут это делать только с помощью собственных секретных ключей, которые зашиты аппаратно.

3.3. Канал утечки в системах на основе криптографии на эллиптических кривых. Известны как минимум два принципиальных подхода к построению лазейки на базе криптографии на эллиптических кривых:

- генерация криптографически слабой эллиптической кривой, построение и публикация изоморфной к ней (изоморфизм является секретным параметром разработчика);
- использование стойкой эллиптической кривой такого вида, что отсутствие проверки того, что точка находится на кривой приводит к переводу операций над классом кривых, в котором разработчик может за приемлемое время решать задачу дискретного логарифмирования.

Идея первого подхода заключается в том, что разработчик сначала выбирает эллиптических кривую E_s, задачу дискретного логарифмирования которой можно свести к задаче дискретного логарифмирования в поле F_2^N, используя определенную функцию спаривания Вейля так, что последняя практически решается разработчиком. Далее, разработчик строит изоморфную кривую E_{pb}, используя секретное преобразование $\varphi : E_s \to E_{pb}$ методом, описанным в [8]. Затем кривая E_{pb} публикуется (например, как часть стандарта) и используется жертвой. В таком случае задача дискретного логарифмирования, например, поиск $x : xG = P$ по известным *G* и *P*, сложная для пользователя системы, однако разработчик может ее свести к задаче на кривой $E_s : P \to \varphi^{-1}(P), G \to \varphi^{-1}(G)$, что сведением к задаче дискретного логарифмирования над полем остатков по методу, описанному в [9] позволяет разработчику решить задачу ECDLP за приемлемое время.

Клептомеханизм второго подхода продемонстрирован на примере схемы цифровой подписи на базе эллиптических кривых ECKCDSA [10]. Идея заключается в том, что в алгоритм генерации цифровой подписи жертвы вводится ошибка (секретный параметр разработчика), что позволяет ему, перехватив определенное количество подписей жертвы, получить ее секретный ключ.

3.4. Каналы утечки секрета в протоколах. Одним из известных примеров таких механизмов является метод SETUP, который позволяет организовать завладение секретным ключом путем преднамеренной модификации реализации криптосистемы на основе задачи

факторизации больших чисел или задачи дискретного логарифмирования в конечных полях. В настоящее время этот метод является теоретическим (общеизвестных фактов его применения не известно), однако вполне реальный для использования на практике. Другой тип атаки – BEAST (CVE-2011-3389) на протокол SSL до версии TLS 1.0, который использует комбинации уязвимостей XSS (Cross Site Scripting) веб сервиса и Session Fixation в реализации CBC режима шифрования протокола SSL. Злоумышленник может принудить жертву выполнить браузерный код таким образом, что в полученной зашифрованной последовательности нарушается уникальность стартового вектора (CBC режим шифра) для каждого открытого сообщения, позволяя нападающему дешифровать секретную часть сообщения. В действительности, маловероятно, чтобы данная атака была спланированным клептографическим механизмом, однако она имеет определенные признаки такого: вследствие вмешательства в систему жертвы образуется канал скрытной утечки секрета.

Заключение

1. Обозначена актуальность нового направления в защите информации – клептографии и ее связь с криптографией и стеганографией.

2. Введено неформальное понятие клептографического механизма как расширение криптосистемы, которое дает дополнительные возможности разработчику.

3. Приведена общая классификация клептографических механизмов.

4. Продемонстрированы некоторые известные криптопримитивы с встроенным клептографическим механизмом.

Список литературы

1. Жуков, А. Криптография и клептография: скрытые каналы и лазейки в криптоалгоритмах / А. Жуков, А. Маркелова // Information Security. – 2019 – № 1 – С. 36–41.

2. Шелест, М. Е. Клептография vs криптография & стеганография / М. Е. Шелест, Б. А. Коваленко, А. И. Трубей // Теоретическая и прикладная криптография : мат-лы междунар. науч. конф., Минск, 20–21 октября 2020 г. Минск, 2021. – С. 106–113.

3. Simmons, G. J. The Prisoners' Problem and the Subliminal Channel [Электронный ресурс] / G. J. Simmons // Advances in Cryptology: Proceedings of Crypto. – Режим доступа : https://doi.org/10.1007/978-1-4684-4730-95.

4. Simmons, G. J. The Subliminal Channel and Digital Signatures [Электронный ресурс] / G. J. Simmons // Advances in Cryptology. – Berlin, Heidelberg: Springer Berlin Heidelberg, 1985:364–378.

5. Kovalenko, B. Kleptography trapdoor free cryptographic protocols [Electronic resource] / B. Kovalenko, A. Kudin // Cryptology ePrint Archive, Report 2018/989. – Режим доступа : https://eprint.iacr.org/2018/989.

6. Young, A. The Dark Side of "Black-Box" Cryptography or: Should We Trust Capstone? / A. Young, , M. Yung // Advances in Cryptology – CRYPTO '96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings / editor N. Koblitz. – Berlin, Heidelberg : Springer Berlin Heidelberg, 1996. – P. 89–103.

7. Biham, E. Differential cryptanalysis of DES-like cryptosystems / E. Biham, A. Shamir // Journal of Cryptology. – 1991. – № 4. –P. 3–72.

8. Galbraith, S. D. Extending the GHS Weil Descent Attack. в: Advances in Cryptology / S. D. Galbraith, F. Hess, N. P. Smart // EUROCRYPT 2002 / editor L. R. Knudsen. – Berlin, Heidelberg: Springer Berlin Heidelberg, 2002. – P. 29–44.

9. Menezes, A. Cryptographic Implications of Hess' Generalized GHS Attack [Electronic resource] / A. Menezes, E. Teske // Cryptology ePrint Archive, Report 2004/235. – Режим доступа : https: // eprint. iacr.org/2004/235. 2004.

10. Bernstein, D. J. How to Manipulate Curve Standards: A White Paper for the Black Hat / D. J. Bernstein, T. Chou, C. Chuengsatiansup // Proceedings of the Second International Conference on Security Standardisation Research. SSR 2015. – Japan : SpringerVerlag, 2015. – P. 109–139.

УДК 003.26.09

СПЕЦИАЛИЗИРОВАННОЕ ИЗДЕЛИЕ ПАК «КЛИЕНТ-ДСП», ПРЕДНАЗНАЧЕННОЕ ДЛЯ ЗАЩИТЫ УДАЛЕННОГО ДОСТУПА В ИНФОРМАЦИОННЫХ СИСТЕМАХ 3-ДСП, 4-ДСП

А.М. САПРЫКИН
ООО «С-Терра Бел», г. Минск, Республика Беларусь

Введение. ООО «С-Терра Бел» работает на рынке Республики Беларусь в сфере сетевых средств криптографической защиты информации (СКЗИ) с 2008 года. Компания разработала и поставляет уже 4-ю по счету линейку Bel VPN продуктов – функционально полного перечня сетевых СКЗИ для обеспечения защиты информационных систем своих пользователей и заказчиков. В их составе: масштабируемые программно-аппаратные и программные шлюзы безопасности, система централизованного управления, модуль шифрования линейного уровня, а также клиенты безопасности под операционные системы Windows и Android, предназначенные для защиты удаленного доступа с отдельных рабочих мест.

Вышеуказанные СКЗИ, выпускаемые под брендом Bel VPN, могут использоваться в защищенных типовых информационных системах любого класса согласно перечню, приведенному в приказе ОАЦ № 66 от 20.02.2020г.

Вместе с тем, в силу специфики законодательства Республики Беларусь для классов 3-дсп и 4-дсп, в частности, согласно Положению о технической и криптографической защите информации, приведенному в Указе Президента Республики Беларусь N 196 от 16.04.2013 в редакции Указа N 449 от 09.12.2019: «*Криптографическая защита служебной информации ограниченного распространения осуществляется только с применением* ***программно-аппаратных средств криптографической защиты***». На практике это означает, что для защиты удаленного доступа в информационных системах классов 3-дсп и 4-дсп с отдельного рабочего места (компьютер, ноутбук, планшет) необходимо использовать программно-аппаратный шлюз безопасности. Его стоимость, как правило, превышает стоимость самого рабочего места. Оборудование получается громоздким и неудобным в использовании. Это, в свою очередь, влечет ограничения в применении, либо полный отказ от использования удаленных рабочих мест в информационных системах классов 3-дсп и 4-дсп.

Описание и характеристики. Комплекс программно-аппаратный (ПАК) «Клиент безопасности Bel VPN Client-ДСП» представляет собой, по сути, мини-шлюз размером со спичечный коробок и весом чуть более 100 граммов. В изделии реализованы взаимосвязанные криптографические стандарты, требуемые для средств линейного шифрования согласно перечню, приведенному в Приказе ОАЦ № 77 от 12.03.2020г.

Клиент-ДСП пройдет испытания на соответствие профилю программно-аппаратных средств криптографической защиты информации, а в его функциях есть также межсетевой экран. Питание Клиента-ДСП возможно как сетевое, так и от порта USB.

Другие характеристики:

- Внутренняя ОС: Debian 10 или Astra Linux
- ОЗУ 1 Гб DDR4;
- 3 x (2 x 10/100/1000 Ethernet + 1 x USB Ethernet).
- производительность до 10 Мбит/с;
- настройка: SSH, Serial;
- централизованное управление с помощью ПП «Bel VPN KP 4.5».
- полная совместимость с Bel VPN продуктами версий 4.1 и 4.5.

Благодаря своей универсальности Клиент-ДСП можно применять для защиты удаленного доступа с рабочих мест, использующих любые операционные системы: Windows, Android, Linux, MacOS и т. п. Интерфейсы подключения: RJ-45 (подключение в разрыв) или USB-Ethernet (on-a-Stick). Предусмотрена как работа с технологическими сертификатами формата РУЦ ГосСУОК, так и на «preshared-key».

Также одним из главных достоинств Клиента-ДСП является его сравнительно невысокая стоимость. В случае применения ПАК Клиента-ДСП полностью исключаются возможные программные конфликты, как это иногда бывает с программными клиентами, например, с антивирусами.

Как представляется, Клиент-ДСП может найти применение не только в типовых информационных системах классов 3-дсп и 4-дсп, но в иных защищенных ИС, где требуется повышенный уровень безопасности, в частности, в платежных терминалах: банкоматах, инфокиосках и других ИС.

Заключение. Новое изделие производства ООО «С-Терра Бел» Клиент-ДСП специально разработано для защиты удаленного доступа в типовых информационных системах классов 3-дсп и 4-дсп. Оно имеет определенные преимущества по сравнению с другими аналогами, предлагаемыми на рынке Республики Беларусь. Выпуск подобного изделия на рынок означает дальнейшее развитие и совершенствование белорусских сетевых СКЗИ в целях наиболее полного удовлетворения запросов потребителей.

УДК 004.056.55

СРАВНИТЕЛЬНЫЙ АНАЛИЗ РАСПРОСТРАНЕННЫХ СИСТЕМ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

М.А. КАЗЛОВСКИЙ
Государственное предприятие «НИИ ТЗИ», г. Минск, Республика Беларусь

Введение. В настоящее время во всем мире активно проводится цифровизация различных сфер жизни общества. В Республике Беларусь, например, в ближайшее время будет проведена выдача идентификационных карт, которые позволят гражданам совершать юридически значимые действия через сеть Интернет. Естественным образом возникает вопрос о создании системы электронного голосования, которая позволила бы избирателям выражать волеизъявление дистанционно.

Использование такой системы имеет ряд неоспоримых плюсов: удешевление стоимости проведения выборов, увеличение процента явки, усложнение фальсификации результатов. Однако, у электронного голосования есть и ряд недостатков, связанных с формой его проведения: сложность удаленной авторизации избирателя, возможность стороннего вмешательства в ход голосования, необходимость в профессиональном аудите как используемых криптографических протоков, так и разработанных программных реализаций.

В работе строится общая модель систем электронного голосования, вводятся требования к таким системам, а также изучается вопрос соответствия известных систем сформулированным требованиям.

1. Субъекты в модели электронного голосования. Как правило, в модели электронного голосования выделяют следующих субъектов: избиратель, кандидат, избирательная комиссия, и противник [1]. Избиратель – субъект, который имеет право голоса и отдает его за одного или нескольких из конкурирующих кандидатов. Избирательная комиссия – это орган, ответственный за проведение выборов. Противник – злонамеренная сущность, которая пытается манипулировать голосованием и/или подсчетом голосов. Внешний противник может воздействовать на избирателя, пытаясь принудить или подкупить его, а также пытаться нарушить конфиденциальность и анонимность избирателей, используя недостатки протокола голосования. Внутренний противник дополнительно может пытаться изменить ход подсчета голосов, раскрыть промежуточные результаты голосования, а также нарушить функционирование избирательной комиссии.

Дополнительно могут быть введены следующие субъекты: регистратор, доска бюллетеней и аудитор. Регистратор осуществляет выдачу бюллетеней избирателям после их аутентификации. Доска бюллетеней – публичное сетевой хранилище зашифрованных бюллетеней с голосами, может быть организована с помощью технологии «блокчейн». Аудитор выполняет контроль за тем, чтобы все остальные субъекты действовали в соответствии с принятым протоколом голосования, не нарушая его.

2. Этапы электронного голосования. Процесс электронного голосования обычно состоит из пяти этапов, при этом этапы 1–4 идут именно в такой последовательности, а этап 5 может выполнятся несколько раз (после каждого из этапов 2–4):

1. Анонс или инициализация, во время которого объявляются используемые протоколы, формируется список избирателей, устанавливаются секретные параметры и назначаются члены избирательной комиссии.
2. Регистрация или аутентификация, во время которой личность избирателя проверяется и подтверждается избирательной комиссией.
3. Голосование, во время которого избиратель отдает свой голос.
4. Подсчет, во время которого избирательная комиссия проверяет валидность голосов и обрабатывает их для подведения итогов выборов.

5. Верификация или аудит, во время которой избиратели и сторонние наблюдатели проверяют отданные голоса.

3. Требования к системе электронного голосования. В качестве базовых свойств, которым должна соответствовать идеальная система электронного голосования, можно выделить:

1. Право голоса (Eligibility): в выборах могут принимать участие только избиратели, которые имеют право голосовать (то есть включенные в список избирателей), при этом избиратель не должен иметь возможность проголосовать больше раз, чем предусматривают правила голосования.

2. Приватность (Privacy): невозможно определить, как проголосовал конкретный избиратель; предполагается что анонимность голоса может быть нарушена только при сговоре избирателя и избирательной комиссии.

3. Корректность (Correctness): все валидные голоса должны быть учтены и подсчитаны, голоса недействительных избирателей не должны быть учтены.

4. Честность (Fairness): чтобы провести беспристрастные выборы, никто не должен иметь возможность подсчитывать промежуточное количество голосов по ходу проведения выборов.

5. Проверяемость (Verifiability): личная (individual) – каждый избиратель имеет возможность убедиться, что его бюллетень учтен корректно и универсальная (universal) – любой желающий имеет доступ к итогам голосования и может проверить, что учтены все действительные бюллетени и подсчет голосов был проведен корректно.

В качестве базовых свойств, которым должна соответствовать идеальная система электронного голосования, можно выделить:

1. Защищенность (Robustness): система должна корректно функционировать даже при активных и пассивных атаках избирателей и/или членов избирательной комиссии, а также при невыполнении или некорректном выполнении субъектом возложенных на него функций.

2. Недоказуемость (Receipt Freeness): избиратель не имеет возможности получить или составить доказательство, подтверждающее содержание его голоса (как именно он проголосовал) – это не позволит заставить избирателя проголосовать определенным образом.

3. Защита от принуждения (Incoercibility): избиратель имеет возможность переголосовать несколько раз в течение всего срока голосования, при это будет учтен только последний голос – это позволит избирателю, находящемуся под контролем противника, проголосовать так, как хочет противник, а после прекращения контроля переголосовать так, как хочет сам избиратель.

4. Криптографические механизмы в системе электронного голосования. В качестве криптографических механизмов, которые могут использоваться в системах электронного голосования можно выделить:

- Протокол аутентификации избирателей: используется для того, чтобы выдать бюллетени только тем избирателям, которые имеют право голосовать.
- Протокол, организующий защищенное соединение: используется для безопасной передачи информации между субъектами системы.
- Шифрование бюллетеней: используется для предотвращения преждевременного раскрытия информации о голосе, содержащемся в бюллетене.
- Отрицаемое шифрование: используется для защиты избирателя от принуждения – он имеет два различных ключа шифрования, при расшифровании которыми бюллетеня будут получены два валидных различных результата.
- Протокол доказательства с нулевым разглашением: используется для подтверждения действительности голоса и/или криптографической операции.
- Протокол конфиденциального вычисления: используется для того, чтобы избиратели могли вычислить результаты голосования, не раскрыв свои голоса.
- Гомоморфное шифрование: используется для обеспечения приватности голосования.
- Протокол слепой подписи: используется для того, чтобы избирательная могла комиссия заверить бюллетень, не узнав его содержимое.
- Протокол разделения секрета: используется для того, чтобы достичь защищенности путем распределения доверия между субъектами.

- Протокол, организующий анонимное соединение (Mixnet): используется для анонимизации голоса избирателя.

Сравнительный анализ некоторых криптографических механизмов приведен в таблице 1.

Таблица 1

Сравнительный анализ некоторых криптографических механизмов

Криптографический примитив	Преимущества	Недостатки
Mixnet	Перемешивание нарушает связи между голосами и избирателями Не требуется фиксированная последовательность этапов	Сообщения имеют большой размер, что снижает эффективность
Слепая подпись	Эффективная и простая реализация	Сложно поддержать универсальную проверяемость
Гомоморфное шифрование	Простая процедура подсчета Невозможно подсчитать количество голосов до начала соответствующего этапа	Восприимчивость к некоторым атакам
Разделение секрета	Повышенная надежность и конфиденциальность	Сложность в реализации Возможные проблемы с масштабируемостью

5. Классификация систем электронного голосования. Все системы электронного голосования можно классифицировать, основываясь на том, как избиратели подают голоса в избирательную комиссию:

- Скрытый избиратель: избиратели подают голоса анонимно [2, 3].
- Скрытое голосование: избиратели открыто подают зашифрованные голоса [4, 5].
- Скрытый избиратель со скрытым голосованием: избиратели отправляют анонимно зашифрованные голоса [6–8].

Рассмотрим также несколько современных систем электронного голосования, представленных в [9]: UVote [10], Zeus [11], Cobra [12], Helios [13], Civitas [14].

6. Сравнительный анализ систем электронного голосования. Сравнительный анализ рассмотренных выше систем проведен в таблицах 2 и 3.

Таблица 2

Сравнительный анализ классических систем электронного голосования

Свойство / схема голосования	[2]	[3]	[4]	[5]	[6]	[7]	[8]
Право голоса	С	С	С	С	С	С	С
Приватность	С	С	С	С	С	С	С
Корректность	С	НИ	С	С	Н	Н	С
Честность	НИ	НИ	НИ	НИ	С	НИ	НИ
Проверяемость	С	ЛП/УП	С	С	ЛП	ЛП	С
Защищенность	Н	НИ	НИ	НИ	Н	НИ	НИ
Недоказуемость	С	С	С	С	Н	С	С
Легенда: С – соответствует, Н – не соответствует; НИ – неизвестно; ЛП – личная проверяемость; УП – универсальная проверяемость							

Таблица 3

Сравнительный анализ современных систем электронного голосования

Свойство / схема голосования	UVote	Zeus	Cobra	Helios	Civitas
Право голоса	С	С	С	С	С
Приватность	С	С	С	С	С
Корректность	С	С	С	С	С
Честность	НИ	С	С	С	С
Проверяемость	ЛП	С	Н	С	ЛП
Защищенность	НИ	С	С	С	С
Недоказуемость	Н	Н	С	Н	С
Легенда: с – соответствует, Н – не соответствует, НИ – неизвестно; ЛП – личная проверяемость					

Заключение. Таким образом, можно сделать вывод, что наиболее перспективными для дальнейшего исследования являются современные системы, в которых скрытый избиратель осуществляет скрытое голосование.

Список литературы

1. Sampigethaya, K. A framework and taxonomy for comparison of electronic voting schemes / K. Sampigethaya, R. Poovendran // Computers & Security. – 2006. – № 25(2). – P. 137–153.

2. Sako, K. Receipt-free mix-type voting scheme – a practical solution to the implementation of a voting booth / K. Sako, J. Killian // Advances in cryptology. EUROCRYPT'95. – Springer-Verlag, 1995. – P. 393–403.

3. Chaum, D. Secret-ballot receipts: true voter-verifiable elections / D. Chaum // IEEE Security & Privacy Magazine. – 2004.

4. Baudron, O. Practical multi-candidate election system. In: Proceedings of the 20th ACM symposium on principles of distributed computing / O. Baudron [et al.]. – ACM Press, 2001. – P. 274–283.

5. Lee, B. Receipt-free electronic voting scheme with a tamper-resistant randomizer / B. Lee, K. Kim // ICISC'02. – Springer-Verlag, 2002. – P. 389–406.

6. Fujioka, A. A practical secret voting scheme for large scale elections / A. Fujioka, T. Okamoto, K. Ohta // Advances in cryptology – AUSCRYPT'92. – Springer-Verlag, 1993. – P. 248–259.

7. Okamoto, T. Receipt-free electronic voting schemes for large scale elections / T. Okamoto // Proceedings of the workshop on security protocols'97. – Springer-Verlag, 1997. – P. 25–35.

8. Aggelos, K. The vector-ballot e-voting approach. In: Financial cryptography / K. Aggelos, Y. Moti. – Springer-Verlag, 2004. – P. 72–89.

9. Li, H. A taxonomy and comparison of remote voting schemes / H. Li, A. R. Kankanala, X. Zou. – ICCCN 2014. – P. 666–673.

10. Abdelkader, R. Uvote: A ubiquitous e-voting system / R. Abdelkader, M. Youssef // Third FTRA International Conference, 2012. – P. 72–77.

11. Tsoukalas, G. From helios to zeus / G. Tsoukalas, K. Papadimitriou, P. Louridas. – Greek Research and Education Network, 2013. – P. 1–10.

12. Essex, A. Cobra: toward concurrent ballot authorization for internet voting / A. Essex, J. Clark, U. Hengartner // Proceedings of the 2012 international conference on Electronic Voting Technology. – 2012. – P. 3–13.

13. Adida, B. Helios: Web-based open-audit voting / B. Adida // Proceedings of the 17th Conference on Security Symposium, 2008. – P. 335–348.

14. Clarkson, M. Civitas: Toward a secure voting system / M. Clarkson, S. Chong, A. Myers. – IEEE Symposium on Security and Privacy, 2008. – P. 354–368.

УДК 621.383

ДОСТОВЕРНОСТЬ ПРИНЯТЫХ ДАННЫХ В КВАНТОВО-КРИПТОГРАФИЧЕСКОМ КАНАЛЕ СВЯЗИ

А.М. ТИМОФЕЕВ
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Введение. Существующие системы квантово-криптографической связи характеризуются максимально высоким уровнем информационной безопасности, что достигается за счет использования квантово-механического ресурса при кодировании передаваемых данных [1, 2]. При этом обмен информацией осуществляется посредством маломощных оптических импульсов, содержащих не более десяти фотонов в расчете на каждый бит (символ). Одной из основных задач, решаемых при построении квантово-криптографических систем связи, является регистрация таких маломощных импульсов. С этой целью целесообразно использовать наиболее высокочувствительные приемные модули – счетчики фотонов [1, 2]. Вместе с тем, особенно важно обеспечивать достаточно высокую достоверность данных, зарегистрированных счетчиками фотонов [3].

Под достоверностью будем понимать вероятность того, что принятые данные соответствуют переданным [3].

Известные методы оценки показателей надежности [4, 5], учитывающие ошибки при передаче информации, не применимы для систем квантово-криптографической связи. В частности, методы, представленные в работах [4, 5], не учитывают мертвое время счетчика фотонов. В течение этого времени счетчик фотонов не чувствителен к падающему на него оптическому излучению, что приводит к ошибкам при передаче данных и к уменьшению достоверности принятых данных [1–3].

В связи с этим целью данной работы являлось установить влияние скорости счета импульсов на выходе счетчика фотонов на достоверность данных, зарегистрированных в квантово-криптографическом канале связи.

Объектом исследования являлся асинхронный двоичный несимметричный однородный однофотонный канал связи без памяти и со стиранием, содержащий в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа. Выбор в качестве объекта исследования такого канала связи обусловлен тем, что его использование не требует наличия дополнительных линий связи для передачи и приема синхроимпульсов [3]. Мертвым временем продлевающегося типа характеризуются счетчики фотонов на базе лавинных фотоприемников, включенных по схеме пассивного гашения лавины [2].

Предметом исследования являлось установить влияние средней скорости счета импульсов при передаче двоичных символов «1» на выходе счетчика фотонов на достоверность зарегистрированных данных.

1. Выражение для оценки достоверности зарегистрированных данных. Дальнейшие рассуждения будут основаны на том, что передача информации осуществляется по квантово-криптографическому каналу связи двоичными символами («0» и «1») в течение длительности времени τ_b. Причем при передаче символов «0» и «1» используются оптические сигналы мощностью W_1 и W_2 соответственно ($W_1 < W_2$), которые содержат от одного до нескольких десятков фотонов и транслируются в линию связи в течение времени однофотонной передачи $\Delta t = \tau_b /2$, а прием – с помощью счетчика фотонов, выполненного на базе лавинного фотоприемника, включенного по схеме пассивного гашения лавины [2]. Следовательно, в течение времени $t_з = \tau_b /2$ данные в канал связи не передаются, т. е. между каждой парой символов находится так называемый «защитный» временной интервал. Поскольку символы «0» и «1» передаются импульсами различной мощности, то на выходе счетчика фотонов за время Δt формируется различное количество электрических импульсов, которое будет прямо пропорционально мощности оптического излучения. Всеми потерями информации, за исключением потерь в счетчике фотонов, пренебрегаем.

Достоверность зарегистрированных данных можно определить на основании соответствующих достоверностей зарегистрированных символов «0» D_0 и символов «1» D_1, полученных в работе [3]:

$$
\begin{aligned}
D = 0{,}5 \times \Bigg\{ & \sum_{N=N_1}^{N_2} \frac{\left[(n_t + n_{s0})(\Delta t - \tau_d)\right]^N \exp\left[-(n_t + n_{s0})(\Delta t - \tau_d)\right]}{N!} \times \\
& \times \Bigg[\sum_{N=N_1}^{N_2} \frac{\left[(n_t + n_{s0})(\Delta t - \tau_d)\right]^N \exp\left[-(n_t + n_{s0})(\Delta t - \tau_d)\right]}{N!} + \\
& + \sum_{N=N_1}^{N_2} \frac{\left[(n_t + n_{s1})(\Delta t - \tau_d)\right]^N \exp\left[-(n_t + n_{s1})(\Delta t - \tau_d)\right]}{N!} \Bigg]^{-1} + \\
& + \Bigg[1 - \sum_{N=0}^{N_2} \frac{\left[(n_t + n_{s1})(\Delta t - \tau_d)\right]^N \exp\left[-(n_t + n_{s1})(\Delta t - \tau_d)\right]}{N!} \Bigg] \times \\
& \times \Bigg[\Bigg[2 - \sum_{N=0}^{N_2} \frac{\left[(n_t + n_{s1})(\Delta t - \tau_d)\right]^N \exp\left[-(n_t + n_{s1})(\Delta t - \tau_d)\right]}{N!} - \\
& - \sum_{N=0}^{N_2} \frac{\left[(n_t + n_{s0})(\Delta t - \tau_d)\right]^N \exp\left[-(n_t + n_{s0})(\Delta t - \tau_d)\right]}{N!} \Bigg] \Bigg]^{-1} \Bigg\},
\end{aligned}
\tag{1}
$$

где N_1 и N_2 – нижний и верхний пороговые уровни регистрации соответственно, n_t – средняя скорость счета темновых импульсов на выходе счетчика фотонов, n_{s0} и n_{s1} – средние скорости счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «0» и «1» соответственно, τ_d – средняя длительность мертвого времени продлевающегося типа.

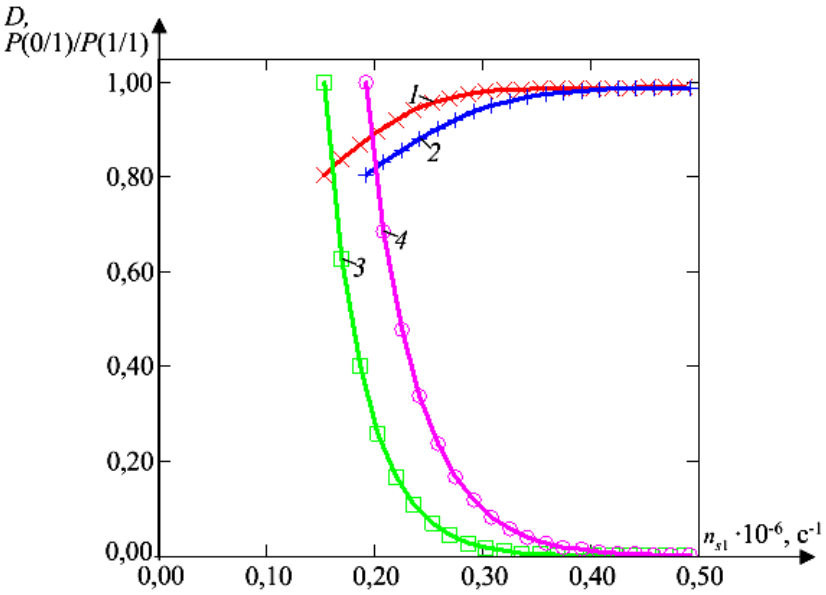
Нижний и верхний пороговые уровни регистрации – это соответственно наименьшее и наибольшее число зарегистрированных на выходе счетчика фотонов импульсов, при котором делается вывод, что передан символ «0». При превышении зарегистрированных импульсов числа N_2 делается вывод, что передан символ «1», а при регистрации импульсов в количестве, меньшем, чем N_1, принимается решение, что символ отсутствует [3].

Темновые и сигнальные – это импульсы, которые появляются на выходе счетчика фотонов соответственно в отсутствии оптического сигнала и в результате воздействия фотонов регистрируемого излучения [2]. Отметим, что для оценки мертвого времени продлевающегося типа используют среднее значение, поскольку его длительность зависит от интенсивности оптического излучения [2].

2. Результаты математического моделирования и их обсуждение. Вычисление достоверности зарегистрированных данных выполнялось для квантово-криптографических каналов связи, содержащих в качестве приемного модуля счетчик фотонов при различных значениях n_{s1} при отсутствии мертвого времени продлевающегося типа, а также при его наличии.

На рисунке 1 представлены зависимости достоверности принятых данных от средней скорости счета сигнальных импульсов n_{s1}.

При построении зависимостей, показанных на рисунке 1, величины средних скоростей счета сигнальных импульсов n_{s0} фиксировались постоянными и выбирались по методике, описанной в работе [3]. При этом критерием оптимальности являлось наименьшее значение n_{s0}, при котором вероятность регистрации на выходе канала связи символов «1» при наличии символов «0» на входе канала связи $P(1/0)$ минимальна [6]. Расчет проводился для одинаковых значений нижнего и верхнего пороговых уровней регистрации $N_1 = 1$ и $N_2 = 7$, средней скорости счета темновых импульсов $n_t = 10^3$ с$^{-1}$ и среднего времени передачи одного бита (символа) $\tau_b = 100$ мкс. Необходимо также отметить, что пороговые уровни регистрации N_1 и N_2 можно выбирать и другими, отличными от 1 и 7, но при сравнении зависимостей $D(n_{s1})$ для различных средних длительностей мертвого времени N_1 и N_2 следует фиксировать



$N_1 = 1$, $N_2 = 7$, $n_t = 10^3$ с$^{-1}$, $\tau_b = 100$ мкс

Рис. 1. Зависимости достоверности принятых данных (кривые *1* и *2*) и отношения $P(0/1)$ / $P(1/1)$ (кривые *3* и *4*) от средней скорости счета сигнальных импульсов n_{s1} при отсутствии мертвого времени (кривые *1* и *3*, $\tau_d = 0$) и при наличии мертвого времени (кривые *2* и *4*, $\tau_d = 10$ мкс)

постоянными, как и среднее значение скорости счета темновых импульсов n_t и среднее время передачи одного бита (символа) τ_b. При этом важно учитывать, что для рассматриваемого канала связи τ_d не может превышать Δt, которое, в свою очередь, должно быть меньше средней длительности передачи одного бита (символа) τ_b на величину защитного временного интервала. В противном случае использование счетчиков фотонов для регистрации данных становится нецелесообразным [3, 6]. Отметим, что при других значениях N_1, N_2, и отношениях $\tau_d/\Delta t$, n_t/n_{s0} и n_t/n_{s1} проявление эффекта мертвого времени продлевающегося типа для рассматриваемого канала связи аналогично представленному на рисунке 1.

Зависимости $D(n_{s1})$ построены в диапазонах средних скоростей счета сигнальных импульсов, на которых вероятности регистрации на выходе канала связи символов «1» при наличии этих символов на входе канала связи удовлетворяют условию [6]

$$P(1/1) \geq 0{,}5. \qquad (2)$$

Из полученных результатов видно, что с увеличением средних скоростей счета сигнальных импульсов n_{s1} зависимости $D(n_{s1})$ растут, достигая насыщения, что имеет место как при наличии мертвого времени, так и при его отсутствии (см. рис. 1, кривые 1 и 2). Причем наличие мертвого времени продлевающегося типа приводит к тому, что это насыщение происходит при больших значениях n_{s1}, чем при отсутствии мертвого времени: при $n_{s1} \geq 35{,}0 \times 10^4$ с$^{-1}$ для $\tau_d = 0$ и при $n_{s1} \geq 43{,}7 \times 10^4$ с$^{-1}$ для $\tau_d = 10$ мкс. Указанные особенности поведения зависимостей $D(n_{s1})$ объясняются характером изменения зависимостей переходных вероятностей $P(1/1)$ и $P(0/1)$ с увеличением средних скоростей счета сигнальных импульсов n_{s1}. Эти зависимости могут быть получены на основании методики [7], поэтому в настоящей работе они не приведены.

Выполненная оценка показала, что с увеличением средней скорости счета сигнальных импульсов n_{s1} вероятность $P(1/1)$ растет вплоть до насыщения, а вероятность $P(0/1)$ уменьшается, тоже переходя в насыщение. Это наблюдается как при наличии мертвого времени продлевающегося типа, так и при его отсутствии. Причем насыщение зависимостей $P(1/1)$ и $P(0/1)$ от n_{s1} происходит при одних и тех же средних скоростях счета сигнальных импульсов n_{s1} для соответствующих средних длительностей мертвого времени продлевающегося типа. Такое поведение зависимостей $P(1/1)$ и $P(0/1)$ с ростом n_{s1} объясняется тем, что статистические распределения смеси числа темновых и сигнальных импульсов на выходе счетчика фотонов при регистрации символов «1» $P_{st1}(N)$ имеют явно выраженный максимум, свойственный распределению Пуассона [2]. При наименьших значениях n_{s1} этот максимум находится между нижним N_1 и верхним N_2 пороговыми уровнями регистрации [8]. В этом случае достаточно велика вероятность $P(0/1)$. С увеличением n_{s1} происходит сдвиг максимумов статистических распределений $P_{st1}(N)$ в сторону больших значений N [8], поэтому переходная вероятность $P(1/1)$ растет, достигая наибольшего значения. В результате в диапазоне n_{s1}, на котором с увеличением

n_{s1} переходная вероятность $P(1/1)$ растет, а переходная вероятность $P(0/1)$ уменьшается, рост зависимости $D(n_{s1})$ объясняется снижением отношения $P(0/1)$ / $P(1/1)$ с увеличением n_{s1} (рис. 1, кривые 3 и 4).

В диапазоне n_{s1}, на котором $P(1/1) \approx 1$ и $P(0/1) \approx 0$, зависимость $D(n_{s1})$ практически неизменна и близка к единице за счет того, что отношение $P(0/1) / P(1/1) \approx 0$ (см. рисунок 1). В диапазонах средних скоростей счета сигнальных импульсов n_{s1}, на которых зависимости $P(1/1)$ от n_{s1} растут, а $P(0/1)$ от n_{s1} уменьшаются, увеличение средней длительности мертвого времени продлевающегося типа при прочих равных параметрах приводит к уменьшению переходных вероятностей $P(1/1)$ и к росту переходных вероятностей $P(0/1)$. Это обусловлено тем, что при увеличении τ_d максимумы статистических распределений $P_{st1}(N)$ сдвигаются в сторону меньших значений N [8]. В результате такого смещения повышается вероятность регистрации на выходе счетчика фотонов импульсов в количестве, меньшем N_2, поэтому $P(1/1)$ уменьшается, а $P(0/1)$ растет. В свою очередь, это приводит, к тому, что на всех исследуемых диапазонах средних скоростей счета сигнальных импульсов n_{s1} при прочих равных параметрах с увеличением τ_d достоверность принятых данных уменьшается за счет роста отношения $P(0/1)$ / $P(1/1)$. В результате, например, при $n_{s1} = 28{,}0 \times 10^4$ с$^{-1}$ достоверность принятых данных D и отношение $P(0/1) / P(1/1)$ равны соответственно $97{,}29 \times 10^{-2}$ и $3{,}17 \times 10^{-2}$ для $\tau_d = 0$; $92{,}76 \times 10^{-2}$ и $14{,}72 \times 10^{-2}$ для $\tau_d = 10$ мкс.

Заключение. Применительно к асинхронному двоичному несимметричному однородному однофотонному каналу связи без памяти и со стиранием, содержащем в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа, установлено, что с ростом средней скорости счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «1» достоверность принятых данных растет, достигая насыщения. Причем при прочих равных параметрах увеличение средней длительности мертвого времени продлевающегося типа приводит к уменьшению достоверности принятых данных, что происходит за счет роста отношения вероятности регистрации на выходе канала связи символов «0» при наличии символов «1» входе канала связи κ вероятности регистрации на выходе канала связи символов «1» при наличии этих символов входе канала связи.

Результаты, полученные в настоящей работе, могут быть использованы при создании систем квантово-криптографической асинхронной связи, позволяющих с высокой достоверностью выявлять несанкционированный доступ к каналу связи за счет уменьшения погрешности определения количества ошибок легитимного приемного оборудования, в качестве которого используются счетчики фотонов с мертвым временем продлевающегося типа.

Список литературы

1. Килин, С. Я. Квантовая криптография: идеи и практика / С.Я. Килин ; под ред. С. Я. Килина [и др.]. – Минск : Бел. наука, 2007. – 391 с.

2. Гулаков, И. Р. Фотоприемники квантовых систем : монография / И. Р. Гулаков, А. О. Зеневич. – Минск : УО ВГКС, 2012. – 276 с.

3. Тимофеев, А. М. Методика повышения достоверности принятых данных счетчика фотонов на основе анализа скорости счета импульсов при передаче двоичных символов «0» / А. М. Тимофеев // Приборы и методы измерений. – 2019. – Т. 10, № 1. – С. 80–89.

4. Дмитриев, С. А. Волоконно-оптическая техника: современное состояние и перспективы / С. А. Дмитриев, Н. Н. Слепов. – 2-е изд., перераб. и доп. – М. : ООО «Волоконно-оптическая техника», 2005. – 576 с.

5. Щеглов, А. Ю. Анализ и проектирование защиты информационных систем. Контроль доступа к компьютерным ресурсам: методы, модели, технические решения / А. Ю. Щеглов. – СПб. : Профессиональная литература, 2017. – 416 с.

6. Тимофеев, А. М. Оценка влияния продлевающегося мертвого времени счетчика фотонов на вероятность ошибочной регистрации данных квантово-криптографических каналов связи / А. М. Тимофеев // Вестник связи. – 2018. – № 1 (147). – С. 56–62.

7. Тимофеев, А. М. Скорость передачи информации однофотонного канала связи с приемным модулем на основе счетчика фотонов с мертвым временем продлевающегося типа / А. М. Тимофеев // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. – 2019. – № 2. – С. 79–86.

8. Тимофеев, А. М. Влияние времени однофотонной передачи информации на вероятность ошибочной регистрации данных асинхронных квантово-криптографических каналов связи / А. М. Тимофеев // Вестник ТГТУ. – 2019. – Т. 25, № 1. – С. 36–46.

ЗАСЕДАНИЕ № 3
СПЕЦИАЛИСТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – ПРОФЕССИЯ БУДУЩЕГО

УДК 004.056.5

О НЕКОТОРЫХ ВОПРОСАХ СОВЕРШЕНСТВОВАНИЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

А.В. МАРЧЕНКО
Начальник отдела 1 управления ФСТЭК России,
г. Москва, Российская Федерация

Уважаемые участники научно-практической конференции!

В условиях широкого внедрения в различные сферы жизни общества современных информационных технологий и как следствия этого нарастающих информационных угроз потребность в высококвалифицированных специалистах по защите информации в органах государственной власти, в организациях производственной сферы, финансово-кредитных организациях, организациях топливно-энергетического сектора экономики, а также в организациях различных форм собственности и других секторов экономики растет.

В последние годы вопросам совершенствования кадрового обеспечения в области информационной безопасности в Российской Федерации уделяется должное внимание.

Указанные вопросы ежегодно рассматриваются на совещаниях и заседаниях, организуемых Советом Безопасности Российской Федерации.

В соответствии с решениями, принятыми на оперативном совещании Совета Безопасности Российской Федерации по вопросу «О кадровом обеспечении безопасности в информационной сфере», Правительством Российской Федерации были даны соответствующие поручения федеральным органам исполнительной власти, направленные на совершенствование кадрового обеспечения в области информационной безопасности.

Поручения предусматривали меры нормативно-правового и организационного характера.

Так, были подготовлены и в настоящее время активно ведется работа по реализации следующих документов:

- Концепция развития кадрового обеспечения в области информационной безопасности в Российской Федерации на долгосрочную перспективу, реализуемая в период с 2017 по 2025 гг.;
- Комплекс мер по формированию прогноза баланса трудовых ресурсов и прогноза подготовки кадров в области информационной безопасности.

На совершенствование кадрового обеспечения в области информационной безопасности направлены принятый и реализуемый федеральный проект «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации», а также решение заседания Межведомственной комиссии Совета безопасности Российской Федерации по информационной безопасности от 27 апреля 2021 г.

В соответствии с запросами, осуществленными в рамках имеющихся полномочий, ФСТЭК России во взаимодействии с Минтрудом России в 2020 году был осуществлен сбор сведений о потребностях в специалистах по защите информации в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления, федеральных фондах, подведомственных им организациях, в организациях оборонно-промышленного комплекса, а также в организациях негосударственного сектора экономики. Анализ представленных сведений показал, что потребность в специалистах по защите информации в указанных государственных органах, фондах

и организациях оборонно-промышленного комплекса составляет около 5000 человек, в свою очередь в организациях негосударственного сектора экономики – около 8000–8500 человек.

На заседании коллегии ФСТЭК России 14 апреля 2021 г. был рассмотрен вопрос «О состоянии и совершенствовании системы подготовки специалистов по технической защите информации и обеспечению безопасности объектов критической информационной инфраструктуры Российской Федерации», где было принято решение по реализации следующих мер в указанной области:

– подготовка предложений по определению контрольных цифр приема по специальностям и направлениям укрупненной группы 10.00.00 «Информационная безопасность» с учетом расширения списка респондентов по запросу сведений о потребности в специалистах по защите информации;

– актуализация примерных программ профессиональной переподготовки и повышения квалификации специалистов по защите информации и разработка новых примерных программ;

– обеспечение разработки примерных программ основных образовательных программ в области информационной безопасности на основе федеральных государственных образовательных стандартов высшего образования, утвержденных в ноябре 2020 г.

ФСТЭК России работу по совершенствованию подготовки специалистов в области технической защиты информации и обеспечению безопасности объектов критической информационной инфраструктуры Российской Федерации проводит в соответствии с полномочиями, наделенными Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

В рамках реализации этих полномочий ФСТЭК России:

– участвует в разработке нормативных правовых актов, регламентирующих сферу образования в области информационной безопасности;

– разрабатывает квалификационные требования к специалистам, работающим в области технической защиты информации и обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации;

– проводит работу по разработке примерных программ дополнительного профессионального образования по вопросам технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, осуществляет рассмотрение и согласование программ подготовки, профессиональной переподготовки и повышения квалификации специалистов по защите информации, представляемых образовательными организациями.

Так, в целях методического обеспечения подготовки специалистов, работающих в области технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры ФСТЭК России разработаны и утверждены три примерные программы профессиональной переподготовки и восемь примерных программ повышения квалификации специалистов по защите информации.

Информация о введении в действие указанных примерных программ доведена до образовательных организаций для использования в подготовке своих рабочих программ профессиональной переподготовки и повышения квалификации.

В связи с вступлением в силу с 1 января 2018 года Федерального закона № 187-ФЗ от 26 июля 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации» ФСТЭК России разработаны и утверждены:

– новая редакция Методических рекомендаций по формированию аналитического прогноза по укомплектованию подразделений по обеспечению безопасности значимых объектов критической информационной инфраструктуры и технической защите информации подготовленными кадрами;

– новая редакция Методических рекомендаций по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры и технической защиты информации.

В целях совершенствования системы подготовки, профессиональной переподготовки и повышения квалификации специалистов по защите информации территориальными орга-

нами ФСТЭК России проводится работа по координации деятельности совещательных органов по подготовке указанных специалистов, созданных в каждом федеральном округе, по вопросам оказания методической помощи образовательным организациям по разработке рабочих программ профессиональной переподготовки и повышения квалификации специалистов по защите информации в соответствие с примерными образовательными программами, утвержденными ФСТЭК России.

При этом необходимо отметить, что ежегодно растет количество образовательных организаций, которые согласовывают с ФСТЭК России свои рабочие программы дополнительного профессионального образования.

Так, в 2019 году таких организаций было 135, в 2020 году – 150 в 2021 году – более 170.

При этом общее количество согласованных с ФСТЭК России рабочих программ дополнительного образования в области информационной безопасности на сегодняшний день более 500, из них программ профессиональной переподготовки – более 100, повышения квалификации – около 400.

В 2021 и 2022 годах ФСТЭК России планируется актуализировать действующие примерные программы профессиональной переподготовки и повышения квалификации, а также разработать и утвердить:

– методические рекомендации по согласованию с ФСТЭК России проектов рабочих программ дополнительного профессионального образования, разработанных образовательными организациями;

– примерную программу профессиональной переподготовки специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры;

– примерную программу повышения квалификации «Техническая защиты информации. Инструментальная и технологическая поддержка проведения фаззингтестирования программного обеспечения».

ФСТЭК России также осуществляет обеспечение образовательных организаций нормативными правовыми актами и методическими документами в области защиты информации.

Во исполнение Комплекса мер по формированию прогноза баланса трудовых ресурсов и прогноза подготовки кадров в области информационной безопасности, ФСТЭК России, начиная с 2016 года, проводит работу по подготовке предложений по определению ежегодных контрольных цифр приема по специальностям и направлениям подготовки укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

Для подготовки указанных предложений по контрольным цифрам приема ФСТЭК России ежегодно осуществляет сбор сведений о текущем состоянии укомплектованности подразделений по защите информации федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, подведомственных им организаций, федеральных фондов, основных кредитно-финансовых организаций, а также организаций оборонно-промышленного комплекса.

Востребованность специалистов в области информационной безопасности обуславливает ежегодное увеличение контрольных цифр приема обучающихся в высших учебных заведениях за бюджетные средства.

Так, рост объема контрольных цифр приема по направлениям подготовки и специальностям высшего образования в данной области составил в 2016 году – 5915, в 2017 году – 6398, в 2018 году – 6642, в 2019 году – 7091, в 2020 году – 7469, в 2021 году – 8654, в 2022 году – 8808.

Общее число обучающихся по образовательным программам бакалавриата, специалитета и магистратуры в области информационной безопасности в 2019 году составило 32 402 человек (в 2018 году – 26 545).

С учетом возрастания угроз и рисков в информационной сфере, значительного внимания к вопросам кадрового обеспечения в области информационной безопасности как со стороны государства, так и со стороны бизнес-сообщества работа по дальнейшему совершенствованию подготовки специалистов по защите информации ФСТЭК России будет продолжена.

УДК 006.089

О РАЗРАБОТКЕ ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е.Б. БЕЛОВ, В.П. ЛОСЬ, Д.И. ПРАВИКОВ
РТУ МИРЭА, Губкинский университет, г. Москва, Российская Федерация

Введение. В Российской Федерации большое внимание уделяется разработке профессиональных стандартов. Считается, что профессиональные стандарты, которые сейчас активно разрабатываются в России, помогут людям стать успешными на рынке труда, откроют доступ к интересной и безопасной работе с достойной оплатой, а работодателям позволят нанять в штат сотрудников, обладающих нужными им компетенциями. Об этом завил глава Минтруда России Антон Котяков, выступая на VI Всероссийском форуме «Национальная система квалификаций России». По состоянию на декабрь 2020 года в России разработано 1500 таких стандартов. Федеральный закон от 03.07.2016 № 238-ФЗ «О независимой оценке квалификации» установил правовые и организационные основы и порядок проведения независимой оценки квалификации работников или лиц, претендующих на осуществление определенного вида трудовой деятельности, а также определил правовое положение, права и обязанности участников такой независимой оценки квалификации. Разработкой профессиональных стандартов охвачены практически все отрасли экономической деятельности государства, в том числе, индустрия информационной безопасности.

1. **Профессиональные стандарты в области информационной безопасности, принятые в 2016 году и подлежащие актуализации.** В 2016 году были утверждены следующие профессиональные стандарты в области информационной безопасности:

- «Специалист по автоматизации информационно-аналитической деятельности»;
- «Специалист по безопасности компьютерных систем и сетей»;
- «Специалист по защите информации в автоматизированных системах»;
- «Специалист по защите информации в телекоммуникационных системах и сетях»;
- «Специалист по технической защите информации».

Необходимость актуализации данных профессиональных стандартов определялась изменениями, произошедшими в методах и средствах защиты информации, а также изменениями в нормативной правовой базе, в частности, в связи с принят ием Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. **Проекты профессиональных стандартов, разработанных в 2020 году.** В 2020 году были разработаны проекты двух новых профессиональных стандартов:

– «Специалист по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

– «Специалист по криптографической деятельности».

Необходимость разработки данных профессиональных стандартов определялась не только изменениями, произошедшими в методах и средствах защиты информации и изменениями в нормативной правовой базе, в частности, в связи с принятием Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», но и все более широким применение средств криптографической защиты информации (СКЗИ) в системах обработки, передачи и хранения информации. Традиционно данные средства применялись исключительно в государственных органах, отвечающих за оборону и национальную безопасность страны. Средства криптографической защиты информации широко используются для обеспечения всесторонней защиты данных, которые передаются по линиям связи.

Анализ государственных и отраслевых нормативных документов, анкетирование работодателей, анализ образовательных программ высшего образования показал, что в настоя-

щее время вопросы криптографической защиты информации изучаются при реализации всех специальностей, связанных с обеспечением информационной безопасности. Востребованность в таких специалистах составляет ежегодно 18 тыс. чел. Все более широкое применение СКЗИ при решении различных задач требует специально подготовленного специалиста в этой области.

Заключение

1. Принятие новых и актуализация действующих профессиональных стандартов будет способствовать становлению системы независимой оценки квалификаций в области информационной безопасности.

2. Уточнение состава профессиональных стандартов важно для конкретизации профессиональных компетенций ФГОС 3++ в области информационной безопасности.

Список литературы

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Федеральный закон от 03.07.2016 № 238-ФЗ «О независимой оценке квалификации».

УДК 004.056.5

ПОДГОТОВКА СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Т.В. БОРБОТЬКО
Белорусский государственный университет информатики и радиоэлектроники, Минск, Республика Беларусь

В соответствии с теорией русского экономиста Н.Д. Кондратьева [1] глубокие изменения в технике и технологиях происходят в фазе экономического подъема, которая обусловлена формированием нового ядра технологического уклада. Информационные технологии в развитии шестого технологического уклада обеспечивают функционирование не только сложных технологических производств, но и являются основой реализацией концепции информационного общества.

Неотъемлемой частью информационной технологии является защита информации [2], которая направлена на обеспечение конфиденциальности, целостности, доступности, подлинности и сохранности сведений. Вместе с тем, развитие методов и способов приема, передачи, сбора и обработки информации, а также доступность их широким массам все больше обостряет проблему информационной безопасности [3]. Таким образом, решение только задачи защиты информации является абсолютно не достаточным сегодня подходом, так как современные методы несанкционированного доступа включает не только техническую составляющую процесса кибератаки, но и социальную инженерию [4], позволяющую повысить эффективность кибератак и увеличить их поверхность. Это в свою очередь предъявляет соответствующие требования к компетенциям, которыми должен обладать специалист, чья деятельность связана с обеспечением информационной безопасности.

В настоящее время в Республике Беларусь сформирована система подготовки кадров в сфере информационной безопасности, которая является многоуровневой и включает первую (срок обучения 4 года) и вторую (срок обучения 1 год 8 месяцев) ступени высшего образования, подготовку научных кадров высшей квалификации, а также курсы повышения квалификации.

Первый уровень системы подготовки кадров по информационной безопасности в Республики Беларусь направлен на формирование кадрового потенциала и обеспечивает подготовку специалистов с высшим образованием, обладающих фундаментальными и специальными знаниями и навыками.

Первая ступень высшего образования в Республике Беларусь по направлению 98 «Информационная безопасность» представлена следующими специальностями:

1. Специальность 1-98 01 01 «Компьютерная безопасность» в рамках, которой, подготовка кадров ведется по двум направлениям: математические методы и программные системы (Белорусский государственный университет, Гродненский государственный университет им. Я. Купалы, Полоцкий государственный университет) и радиофизические методы и программно-технические средства (Белорусский государственный университет, Витебский государственный университет им. П.М. Машерова, Гомельский государственный университет им. Франциска Скорины);

2. Специальность 1-98 01 02»Защита информации в телекоммуникациях» (Белорусский государственный университет информатики и радиоэлектроники). По данной специальности подготовка ведется, в том числе и на английском языке;

3. Специальность 1-98 01 03 «Программное обеспечение информационной безопасности мобильных систем» (Белорусский государственный технологический университет).

Важным аспектом при подготовке специалистов по информационной безопасности является наличие в учебном плане специальности дисциплин, которые обеспечивают формирование профессиональных компетенций в области противодействия информационно-психологическому воздействию на социотехнические системы.

Вторая ступень высшего образования обеспечивает формирование знаний и навыков научно-педагогической и научно-исследовательской работы и в Республике Беларусь представлена специальностью 1-98 80 01 «Информационная безопасность». Обучение проводится по следующим профилям специальности:

1. Защита информации в информационных системах (Белорусский государственный университет информатики и радиоэлектроники);

2. Методы и средства защиты информации в инфокоммуникациях (Белорусский государственный университет информатики и радиоэлектроники) – обучение на английском языке;

3. Аппаратно-программные средства защиты информации (Белорусский государственный университет).

Для изучения, обобщения и распространения педагогического опыта учебной, воспитательной и учебно-методической работы педагогических работников учреждений высшего образования, а также разработке рекомендации по совершенствованию образовательного процесса, организации обмена опытом между учреждениями высшего образования создано учебно-методическое объединение по образованию в области информатики и радиоэлектроники при Учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Подготовка научных кадров высшей квалификации обеспечивается по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность». Для обеспечения процесса подготовки кадров в Республике Беларусь действует два докторских совета по защите диссертаций при Белорусском государственном университете информатики и радиоэлектроники (Д 02.15.06 – по техническим наукам) и Белорусском государственном университете (Д 02.01.02 – по техническим и физико-математическим наукам). Данное направление в подготовке кадров является значимым для пополнения коллективов университетов, научно-исследовательских и других организаций высокопрофессиональными кадрами, которые в том числе будут принимать непосредственное участие в подготовке кадров для обеспечения системы национальной безопасности Республики Беларусь.

Третий уровень системы подготовки кадров по информационной безопасности в Республики Беларусь представлен курсами повышения квалификации, успешное прохождение которых является одним из обязательных условий получения специального разрешения (лицензии) на деятельность в сфере информационной безопасности. В соответствии с [5] проведение курсов повышения квалификации обеспечивается Республиканским унитарным предприятием «Национальный центр обмена трафиком». Повышение квалификации, в соответствии с требованиями законодательства в сфере информационной безопасности необходимо проходит не реже одного раза в три года собственниками (владельцами) информационных систем и владельцами критически важных объектов информатизации.

Данное направление является одним из видов профессионального обучения работников предприятий, которое проводится с целью повышения уровня теоретических знаний, совершенствования практических навыков и умений сотрудников организации с учетом современных требований к их квалификации.

Вместе с тем, необходимо отметить, что тот период времени, который отводится на освоение программы курсов повышения квалификации, не может рассматриваться как формирование фундаментальных знаний. В настоящее время реалии жизни таковы, что должности специалистов по защите информации занимают люди, которые не имеют профильного образования по специальностям направления 98 «Информационная безопасность». Отсутствие системных знаний у таких людей, не позволяет им решать важнейшие задачи для организаций в области информационной безопасности и в конечном итоге приводит к инцидентам.

Решение данной проблемы требует наличия соответствующих нормативных правовых актов, которые юридически определили бы сущность такого процесса как переподготовка по информационной безопасности специалистов с высшим техническим образованием в зону ответственности которых входит обеспечение информационной безопасности или защиты информации, не ограничиваясь лишь курсами повышения квалификации. Здесь важным является и обучение руководителей организаций, которым приходится также принимать соот-

ветствующие решения. Необходимость переподготовки также обусловлена, тем, что квалифицированный специалист по защите информации способен реализовать обучение пользователей информационных систем, что определено в соответствующем положении [6].

Совершенствование системы подготовки кадров также затрагивает проблему повышения качества подготовки специалистов по информационной безопасности. Это в свою очередь требует разработки и практической реализации системы мер, направленных на работу со школьниками, что позволит ориентировать молодежь на осознанный выбор будущей профессии. Так, например, в Учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» в рамках «Академии информатики для школьников» открыто направление «Кибербезопасность», где проводится обучение школьников 7-11 классов. Программа подготовки включает два модуля: базовый «Безопасность персональных данных» и углубленный «Безопасность информационных сетей», целью которых является получение знаний и практических навыков по обеспечению безопасности информации, которая хранится, обрабатывается и передается с помощью средств вычислительной техники.

Необходимо отметить, что система подготовки кадров в области информационной безопасности в Республике Беларусь является зрелой и обеспечивает непрерывную подготовку специалистов по схеме первая ступень высшего образования – вторая ступень высшего образования (магистратура) – аспирантура – докторантура – курсы повышение квалификации. Ее совершенствование требует в первую очередь принятия нормативных правовых актов, которые бы определили необходимость прохождения переподготовки для лиц, в должностные обязанности которых входят вопросы обеспечения информационной безопасности, включая руководящих работников. Кроме того, значимым является формирование целевого набора в университеты на специальности направления 98 «Информационная безопасности» и соответствующей профориентационной работы со стороны университетов со школьниками.

Список литературы

1. Большие экономические циклы // Портал экономистъ – экомика, финансы, экономические науки [Электронный ресурс]. – 2020. – Режим доступа : https://economuch.com/osnovyi-ekonomiki/183-bolshie-ekonomicheskie-32384.html – Дата доступа : 21.04.2021.

2. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации».

3. Концепция национальной безопасности Республики Беларусь, утвержденная Указом Президента Республики Беларусь № 575 от 9 ноября 2010 г.

4. Борботько, Т.В. Трансформация модели нарушителя Cyber Kill Chain при современном уровне развития информационных технологий / Т.В. Борботько // Комплексная защита информации: Мат. XXV науч.-практ. конф. / Москва: Медиа Группа «Авангард», 2020. С. 80-83.

5. Постановление Совета Министров Республики Беларусь от 3 апреля 2020 г. № 204 «О повышении квалификации по вопросам технической и (или) криптографической защиты информации».

6. Положение о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденное Приказом Оперативно-аналитического центра при Президенте Республики Беларусь № 66 от 20 февраля 2020 г.

УДК 004.056

АКТУАЛЬНЫЕ ВОПРОСЫ РАЗВЕРТЫВАНИЯ СИСТЕМЫ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЦИОТЕХНИЧЕСКИХ СИСТЕМ В УСЛОВИЯХ ПОСТРОЕНИЯ ГЛОБАЛЬНОЙ ИНФОРМАЦИОННОЙ ЭКОНОМИКИ

В.Р. ГРИГОРЬЕВ
Институт комплексной безопасности и специального приборостроения, РТУ МИРЭА, г. Москва, Российская Федерация

В настоящее время в ходе осуществления 4-ой технологической революции происходит глобальный процесс коренных преобразований по становлению нового уклада мировой экономики и нового цифрового коммуникационного пространства. По-сути мир переходит к новому «цифровому мышлению», являющемуся следствием кардинальных изменений в среде обитания человека. От постиндустриального мира человечество входит в новую информационную эпоху, связанную с построением информационного общества и информационной экономики, основой которых являются не материальные ресурсы, что было свойственно хозяйственному укладу всех предыдущих социально-экономических формаций, а новая среда сосуществования, которая будет базироваться на виртуальном ресурсе, коим является информация.

Президент РФ В.В.Путин в Послании Федеральному Собранию в 2018 году отметил: «В мире сегодня накапливается громадный технологический потенциал, который позволяет совершить настоящий рывок в повышении качества жизни людей, в модернизации экономики, инфраструктуры и государственного управления. Насколько эффективно мы сможем использовать колоссальные возможности технологической революции, как ответим на ее вызов, зависит только от нас. И в этом смысле ближайшие годы станут решающими для будущего страны. Подчеркну это: именно решающими… Дело в том, что скорость технологических изменений нарастает стремительно, идет резко вверх. Тот, кто использует эту технологическую волну, вырвется далеко вперед. Тех, кто не сможет этого сделать, она – эта волна – просто захлестнет, утопит».

Такая «технологическая волна» построения глобальной информационной экономики информационного общества остро ставит вопрос об обеспечении уже не просто комплексной безопасности, включающей по совокупности отдельные направления защиты субъектов информационной инфраструктуры на всех ее уровнях, а о формировании целостной синергетической информационной безопасности всей социотехнической инфраструктуры как единого объекта защиты, так как «цифровое общество» базируется не просто на «цифре», а на цифровом измерении всех жизненно важных функций как отдельного человека, так и человеческого сообщества и государства как таковых в целом.

Развитие новой синергетической отрасли информационной среды жизнедеятельности человека в виде взаимосвязанных объектов защиты (рис. 1): «цифровой экономики» (ЦЭ), «цифрового социума», интернета вещей, «критических информационных инфраструктур», других промышленных и бытовых киберфизических систем требует, очевидно, развертывания масштабной подготовки грамотных, профессионально подготовленных специалистов в области ИТ цифровой экономики и социо-киберфизических систем и, прежде всего, в области обеспечения информационной безопасности (ИБ).

Совершенно очевидно, что само понятие ЦЭ означает перевод экономических и финансовых инструментов организации и ведения эффективной экономики в виртуальную область цифровых технологий. А, следовательно, углубляются как традиционные проблемы защиты информации (ЗИ), как то «защита аппаратно-программных платформ» от компьютерных атак в части нарушения конфиденциальности, целостности и доступности, функциональной устойчивости, так и возникают новые информационные угрозы, направленные на сознание человека и сообщества в целом. Ясно, что ЦЭ, основываясь на криптографии, по-

требует роста необходимости массовой подготовки специалистов в области открытой криптографии, а также специалистов в области прикладного программирования и искусственного интеллекта. Технологии blockchain и bitcoin позволяют взглянуть по-новому на такие фундаментальные понятия, как ценообразование, соотношение цифровых и бумажных валют, меры юридического доверия и т. д. То есть в корне будут пересмотрены основы традиционной монетизированной «бумажной» экономики.

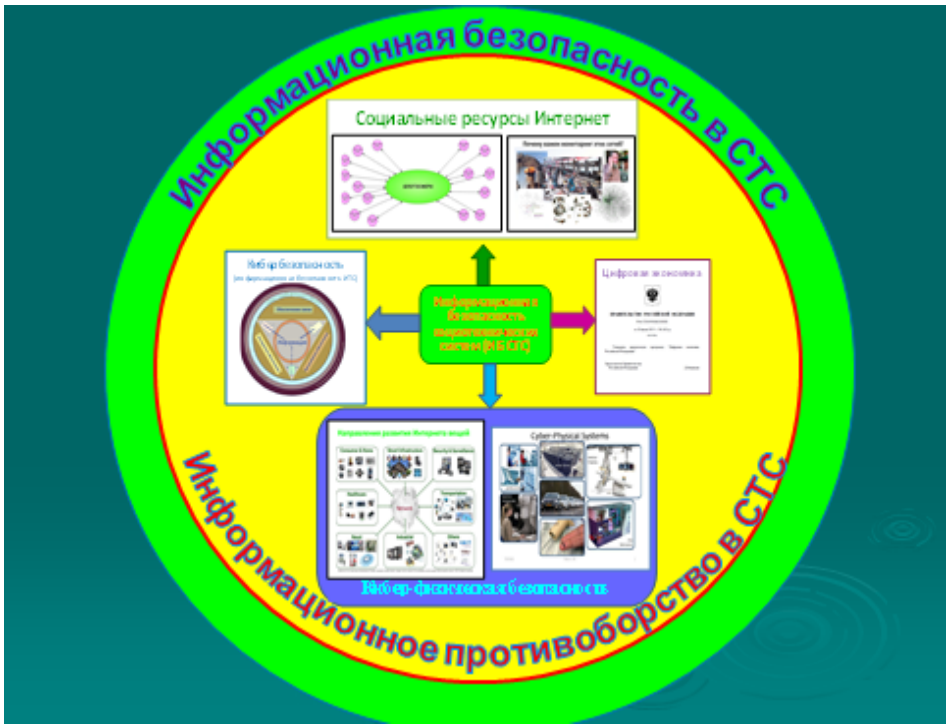


Рис. 1. Схема обеспечения синергетической информационной безопасности всей социотехнической инфраструктуры как единого объекта защиты

Вопросы защиты информации в области киберфизических систем актуальны сегодня во всем мире. Тема важна для развития конкурентоспособного технологического бизнеса в России, особую важность она приобретает в связи с реализацией Программы «Цифровая экономика». Подготовка специалистов для этой бурно растущей отрасли является важным условием в решении проблем, стоящих перед российским технологическим рынком в части нормативно-технического регулирования перспективных технологий: интернета вещей, больших данных, умных городов и других.

Более того, в настоящее время речь идет о создании систем защиты более широкого класса «социо-киберфизических систем» – нового (термин Cyber Physical System (CPS) появился в 2006 году), но перспективного инновационного направления. CPS – это системы, состоящие из различных природных объектов, искусственных подсистем и управляющих контроллеров, которые представляют собой единое целое. Добавление «social» подразумевает вовлечение в эту систему человека и общества. Предпосылками появления таких сложных механизмов принято считать освоение наукой и промышленностью различных вычислительных, автоматизированных и сенсорных систем. Отличие CPS состоит в том, что они подразумевают тесное взаимодействие технологий с физическими ресурсами: социо-киберфизические системы основаны на инженерном моделировании и способны адаптироваться к изменениям окружающей среды.

Таким образом, необходимо констатировать, что создание программно-аппаратных платформ ЦЭ, Интернета вещей, в свою очередь, тесно связаны с социальными коммуникационными возможностями Интернет. Особенность обеспечения ИБ в таких системах состоит в том, что информационно-гуманитарное деструктивное воздействие, в отличие от информационно-технического деструктивного воздействия, направлено не на программно-аппаратные платформы используемых информационно-коммуникационных систем, а предполагает использование ИКТ и специально подготовленной информации для воздействия на

личность, общество и государство в явном и закамуфлированном виде. Объектом информационно-гуманитарного деструктивного воздействия является сознание общества (его части), определенных выделенных социальных (этнических, конфессиональных и др.) групп и отдельных индивидов. Среди инструментов, используемых для оказания деструктивного информационно-гуманитарного воздействия можно выделить современные электронные средства массовой информации и социальные компьютерные сервисы, функционирующие в глобальном информационном пространстве. При этом непосредственно воздействие осуществляется с использованием методов (в том числе, компьютерных) психологии, социологии и социальной инженерии посредством использования специальным образом препарированного содержания (контента) информационных сообщений.

Сегодня, очевидно, что спектр проявления информационных угроз в области ЦЭ значительно шире, чем компьютерные угрозы. Это, прежде всего, имиджевые угрозы бизнесу как таковому, так и ЛПР, задействованных в ключевых отраслях цифровой экономики. Социальная инженерия получит новый импульс в части сбора компрометирующих материалов в социальных ресурсах Интернет, а также будут активно развиваться новые методы и технологии распространения специально подготовленной деструктивной информации (цифровых слухов), порочащей честь и деловую репутацию как юридических, так и физических лиц.

В этом отношении, для адекватой подготовки специалистов «цифровой эры», безусловно, важно задействовать имеющийся в российских вузах потенциал в части подготовки специалистов гуманитарного профиля. Создаваемая организационная структура (профильные кафедры) должна быть стратегически ориентирована на подготовку специалистов новой формации, синтетически объединяющей фундаментальные основы подготовки специалистов технического профиля с современными базисными знаниями основ практической компьютерной психологии, социологии и социальной инженерии.

Таким образом, выделенные проблемы обеспечения информационной безопасности в социотехнических системах (СТС), тесно связанные между собой, определяют и направления подготовки специалистов, которые уже сейчас становятся востребованными в бурно развивающемся цифровом пространстве социального, экономического и финансового взаимодействия в многоагентных сетевых многосвязных структурах формирующегося глобального цифрового общества.

Анализ текущего состояния и перспектив обеспечения информационной безопасности России показывает, что важнейшим, определяющим всю проблему в целом, фактором является целенаправленная подготовка высококвалифицированных кадров, способных эффективно решать постоянно увеличивающийся комплекс задач по гарантированной защите современных телекоммуникационных и информационных технологий, составляющих инфраструктуру информационного базиса государственных систем управления. Информационная безопасность России во многом определяется именно стратегией подготовки специалистов в области новых информационных технологий, определяющих независимость государства с точки зрения своевременного адекватного ответа на стратегические вызовы в XXI веке. Требования, которые предъявляются новому поколению специалистов, существенно возрастают в силу беспрецендентной сложности указанных задач при постоянном росте внешних и внутренних угроз информационной безопасности России.

Как показывает опыт США, даже в этой стране, собравшей “цвет” специалистов по информатике из многих государств, внедрение надежной защиты в современные телекоммуникационные технологии отстает от создания и ввода в эксплуатацию собственно самих технологий современных информационно-телекоммуникационных систем. Кроме того, имеется тенденция к расширению круга задач, требующих неотложного решения с позиций защиты информации (например, противодействие «информационному оружию», защита критических государственных и экономически значимых инфраструктур, разработка конверсионных технологий двойного назначения и т. д.).

Все это определяет актуальность проблемы улучшения организации процесса подготовки и переподготовки специалистов в данной области как задачу государственной важности. Но, к сожалению, следует отметить, что ни один вуз в РФ не ведет целенаправленно подготовки специалистов в этой бурно развивающейся области.

В связи с чем становится крайне актуальной задача своевременного оперативного перестраивания всего процесса подготовки и обучения специалистов в Российской Федерации с адаптацией его к новым требованиям времени и спроса потенциальных заказчиков из госструктур, промышленности, академического сообщества, бизнеса и финансовых структур.

В настоящее время Федеральное учебно-методическое объединение в сфере высшего образования по УГСН 10.00.00 Информационная безопасность (далее – ФУМО ВО ИБ) охватывает вузы, готовящие специалистов только в области обеспечения информационно-технической безопасности. Задачи, определенные Доктриной информационной безопасности РФ в области информационно-психологической и информационно-духовной безопасности, не входят в зону компетенции этого ФУМО. Соответственно, для этих сфер ИБ нет ни образовательных, ни профессиональных стандартов (рис. 2).

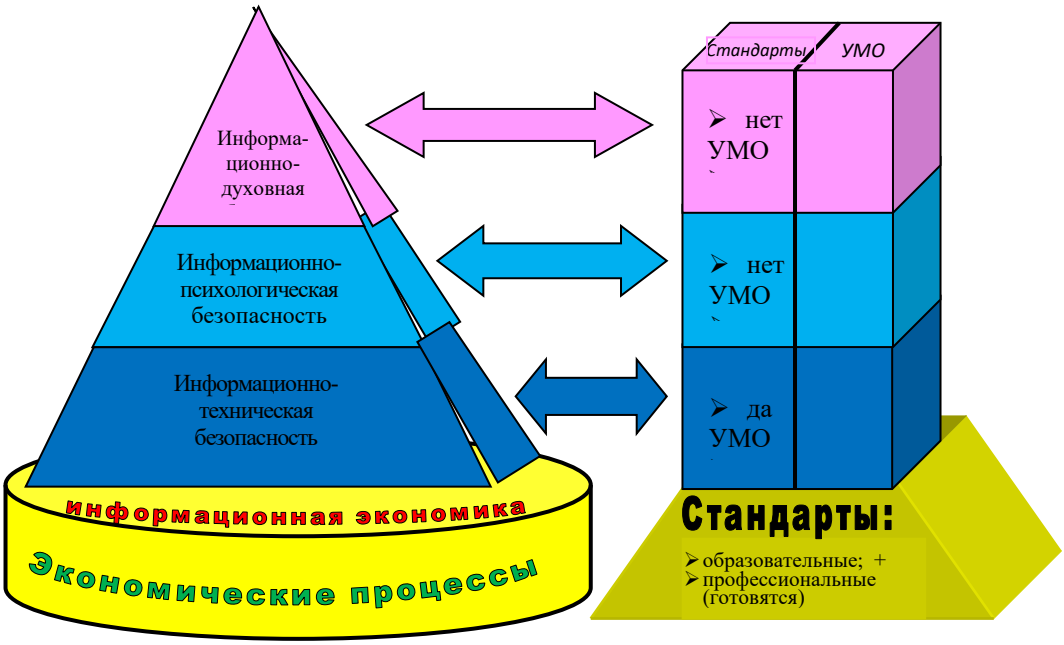


Рис. 2. Классификация составляющих информационной безопасности
в зависимости от характера обрабатываемой информации

В этой связи возможно 2 варианта развития ситуации:

1) связан с расширением компетенций существующего ФУМО ВО ИБ и образования в нем, соответственно, нового отделения по вопросам ИБ СТС;

2) связан с созданием самостоятельного ФУМО ВО ИБ СТС, что, как представляется, в большей степени соответствует специфике обеспечения защиты таких объектов, как общественное, групповое и индивидуальное сознание от деструктивных факторов информационного воздействия через СМИ и другие каналы воздействия.

Первоочередными задачами на ближайшее время можно определить следующие:

– создание номенклатуры новых специальностей в области ИБ СТС;

– образование профильных Учебно-методических советов по специальностям, входящих в пул специальностей по направлению подготовки «Информационная безопасность социотехнических систем»;

– разработка новых федеральных государственных образовательных стандартов высшего профессионального образования по направлению подготовки «Информационная безопасность социотехнических систем» (квалификация (степень) бакалавр и магистр);

– разработка при участии МОО «Ассоциация защиты информации» профессиональных стандартов по группе занятий (профессий) «Специалисты в области информационной безопасности социотехнических систем». Эти профессиональные стандарты должны отражать современные квалификационные требования работодателей и будут использоваться для подготовки профессионально подготовленных кадров, их оценки (сертификации), должностных инструкций, тарификации и пр.

УДК 371.214.6

РЕАЛИЗАЦИЯ В МГЛУ НОВЫХ СТАНДАРТОВ ОБУЧЕНИЯ ПО СПЕЦИАЛЬНОСТИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

А.П. КУРИЛО

Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный лингвистический университет», г. Москва, Российская Федерация

Министерством науки и высшего образования Российской Федерации разработаны и утверждены два новых федеральных образовательных стандарта для подготовки специалистов в области информационной безопасности: 10.03.01 и 10.04.01. В новом учебном году ВУЗЫ начинают учить студентов по программам, разработанным по этим стандартам.

МГЛУ, каки другие заинтересованные и причастные ВУЗЫ, активно работает над реализацией этих ФГОС и подготовкой качественных образовательных программ. Как оказалось, возможности разработки ОПОП применительно к профилю подготовки, выбранному ВУЗОМ рамках этих ФГОС достаточно невелики из-за имеющихся ограничений, однако возможны. Естественно, раз возможны, возникает вопрос о целях, целесообразности и результатах такого маневра.

Определяющим фактором тут является запрос рынка. Информация о том, кто нужен рынку сейчас и в некоторой перспективе имеется у практикующих специалистов. Они уже длительное время отмечают постоянно растущий дефицит специалистов, растущую потребность в них. Более того, в последнее время почти все организации заявляют об возрастающем растущем числе вакансий с одной стороны и весьма низком уровне квалификации приходящих на рынок специалистов с другой. По общему мнению, выпускники ВУЗОВ необходимо доучивать. Но задача это не благодарная, как правило, после приобретения необходимой квалификации они оставляют место работы в погоне за более высокой зарплатой, а возможности закрепить их на работе там, где их доучивали, нет. Поэтому как правило, фирмы не ведут такую работу. Естественным при этом становится завышение специалистами, имеющими необходимую квалификацию, требований по зарплате. В свою очередь, выдержать таких дорогих специалистов в современных реалиях может далеко не каждая фирма. Результат – монополизм, отсутствие конкуренции, сжатие рынка. То есть, практический результат обратен целям, провозглашаемым руководством страны.

Уместны вопросы:

- специалисты с какими компетенциями нужны рынку?[1]
- выпускают ли ВУЗЫ специалистов с требуемыми компетенциями?
- что улучшить в учебном процессе?
- как организовать учебный процесс в рамках ФГОС?
- какими силами организовать учебный процесс?

А пока рынок в массовом порядке отмечает низкую квалификацию выпускаемых специалистов.

Проблема это многогранная. Сама проблематика информационной безопасности демонстрирует быструю изменчивость и вариативность. Изменения в проблематике и новые направления возникают настолько быстро, буквально в течение 2х-3х лет, что образовательные учреждения не успевают за ними, адаптация ФГОС и ОПОП отстает от практики, в результате чего не происходит научного и методологического осмысления возникающих вопросов. И еще раз подчеркну, что практический опыт и знания и в этой сфере накапливаются у практикующих специалистов. Как донести эти знания до студентов и превратить в их компетенции?

---

[1] По данным экспресс-опроса:способность разрабатывать и проектировать информационные системы и СОИБ, с использованием основных наиболее распространенных информационных средств и систем и систем защиты информации; работа на первой линии операторов SOC;работа в группах реагирования и разбора инцидентов.

На какой учебно-материальной базе готовить студентов, когда ФГОС устанавливает только самые общие требования к ней. Но для того, чтобы подготовить из студентов специалистов, владеющих упомянутыми выше компетенциями, нужна специализированная и довольно дорогостоящая материальная база. Где и как ее взять, кто заинтересован, в том, чтобы она была развернута в ВУЗАХ. На этот вопрос необходимо ответить.

Преподаватели ВУЗОВ, как и любой человек, нацелены на повышение своей зарплаты. Это возможно до известных пределов, однако требует полной учебной нагрузки, ведения деятельности по получению ученых степеней и званий, написанию большого числа статей в индексируемые журналы и т. д. к тому же они перегружены отчетностью. Все это практически исключает для них возможность повышения профессиональной компетенции путем участия в работах по решению наиболее острых вопросов практической деятельности в области ИБ. Поэтому ФГОС благосклонно сморит на привлечение к работе практикующих специалистов. Но возникает вопрос: как их привлечь, какую «морковку» повесить перед ними, чтобы привлечь к преподаванию в высшей школе? Работать с серьезной учебной нагрузкой они не могут по причине занятости на основной работе, да и часто не имеют практики преподавания, не говоря об ученых степенях и званиях. Плохо также с публикациями. Составление учебных программ и разработка учебных пособий превращается в муку для них и методистов кафедр. А те небольшие часы, которые они тратят на преподавание, оплачиваются по общим тарифам. Вот и получается, что ведущие специалисты-практики получают за передачу своих очень важных знаний студентам сущие копейки, вызывающие разве что смех. Далеко не каждый готов работать в таких условиях.

На этом фоне платные учебные заведения, занимающиеся в основном подготовкой специалистов по специализированным учебным программам, выглядят гораздо мобильнее и при этом платят приглашенным преподавателям с рынка как минимум в три раза больше. При этом, обязательной бумажной отчетности преподавателей там практически нет. И туда идут люди.

Весьма не просто обстоят дела с практикой. Платное специализированное повышение квалификации с выдачей соответствующего, признаваемого рынком сертификата, есть, а вот практика студентов – есть проблемы. Задача организации практики в современных реалиях весьма сложна. Министерство ужесточает требования к ее прохождению, фактически теперь практику старших курсов нельзя проводить в самом учебном заведении, нужно договариваться с рынком. Однако на рынке далеко не все профильные организации горят желанием принимать практикантов, а если и принимают, то с прицелом подобрать кандидатов на работу. Вызывают вопросы сам процесс прохождения практики, он требует организации и сопровождения практикантов, работы с ними, что требует привлечения ресурсов на обеспечение этой деятельности. Крайне сложно выстраивается формальная сторона вопроса, начиная с подписания договоров, которое превращается в «дуэль юристов», отнимающую время, которого и так не много. В целом, организация практики – тяжелый процесс, занимающий львиную долю времени преподавателей и организаторов.

Вместе с тем, по мнению и преподавателей, и принимающих сторон, практика – это ключевой элемент практической подготовки будущих специалистов. Уместно задать вопрос: а каков практический результат этой деятельности в складывающихся условиях и как ее радикально улучшить. Ответ не радует. И, пожалуй, главное- это сложность привлечения к сотрудничеству коммерческих фирм, они не видят и не ощущают своей заинтересованности в этом процессе. А государство, ужесточающее требования к ВУЗАМ в этой части, не включило рынок в состав заинтересованных субъектов.

Вцелом, эти факторы крайне негативно влияют на общую ситуацию. Поневоле на ум приходит сравнение с тяжелой опасной болезнью, признаки которой сначала не видны, но именно в это время ее можно вылечить. Потом поздно. Ничего не помогает.

Нельзя сказать, что эту ситуацию не видит уважаемое сообщество, разрабатывающие идеологию обучения специалистов в области информационной безопасности. Видит и пытается решать. Появилась новация: сопряжение компетенций выпускников, сформулированных на основании ФГОС, с трудовыми функциями, определенными профессиональны-

ми стандартами, разрабатываемыми уже Минтруда. Такие стандарты появились в 2016 году. Значит, разрабатывать их начали примерно в 2012–2014г.г. По факту, 7–9 лет назад. За это время практика убежала далеко вперед, стандарты явно устарели. С этой проблемой мы в МГЛУ явно столкнулись при разработке новых ОПОП по новым шаблонам, присланным из Минобра. Выходов из этой проблемы два: либо формализация, что еще дальше ухудшает проблему, либо творческая переработка поставленной задачи, по которой мы пошли. Вообще представляется, что интенсивная детализация процесса обучения и его последующая стандартизация, может стать опасным явлением. Ведь стандартизация, если вернуться к сути этого процесса, предназначена для закрепления типовых и отработанных действий, условий или требований, приводящих в итоге к обеспечению единого, стандартного уровня качества выпускаемой продукции или предоставляемых услуг.

Я уже не говорю о том, что информационная безопасность – это не строгая математическая дисциплина, а целая практическая отрасль, опыт и знания в которой возникает у практикующих специалистов «на кончиках пальцев». отрасль с колоссальным числом разного рода ответвлений и направлений, от исследований кода и программирования, до вопросов анализа уязвимостей, трассировки атак и социальной инженерии. В целом, она поразительно в этом смысле напоминает медицину. Но там система подготовки специалистов существенно другая.

Заключение

1. ВУЗАМ, для подготовки специалистов в соответствии с выбранным профилем подготовки, нужна специализированная учебно-материальная база. Как ее создать – вопрос обсуждения с Минобром.

2. Система оплаты работы преподавателей, привлекаемые с рынка, должна быть изменена. Оплату их работы следует осуществлять не по стандартной почасовой ставке, а по договору, «за курс» как это и было ранее, в 90-е годы прошлого века. Но при этом, договорная цена должна быть конкурентоспособна с аналогичными коммерческими курсами.

3. Длительность производственной практики для студентов должна быть существенно увеличена. Один из вариантов – создание в профильных фирмах, выбранных на основании договоров между ВУЗАМИ и коммерческим фирмами о создании учебных консорциумов, определенного числа временных рабочих мест за счет государства, коль скоро оно заинтересовано в повышении уровня образования специалистов в области информационной безопасности.

УДК 378.046.4

О ПРАКТИКЕ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.Н. ЛЕПЕХИН, И.В. МЯЧИН
Оперативно-аналитический центр при Президенте Республики Беларусь
г. Минск, Республика Беларусь

Информационное общество, к которому неуклонно стремится все человечество, коренным образом изменило статус информации. Информационная сфера превращается в системообразующий фактор жизни людей, обществ и государств. Усиливается роль и влияние средств массовой информации, а также глобальных коммуникационных механизмов на экономическую, политическую и социальную ситуацию. Информационные технологии нашли широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями. Происходит эволюция информационного противоборства как новой самостоятельной стратегической формы глобальной конкуренции. Распространяется практика целенаправленного информационного давления, наносящего существенный ущерб национальным интересам. Известное выражение Натана Майера Ротшильда «кто владеет информацией, тот владеет миром» [1] показывает, как те, кто владеет наибольшим объемом информации по какому-либо вопросу, могут деформировать механизмы коммуникации и дестабилизировать функционирование основных систем общества. Именно поэтому на первый план в современном обществе выходит проблема информационной безопасности. При этом, согласно Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575, под информационной безопасностью понимается состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [2].

Концепцией информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 определено, что целью обеспечения информационной безопасности является достижение и поддержание такого уровня защищенности информационной сферы, который обеспечивает реализацию национальных интересов Республики Беларусь и ее прогрессивное развитие.

Обеспечение информационной безопасности осуществляется в соответствии с государственной политикой в данной области, которая включает в себя формирование, совершенствование и реализацию организационных, правовых, научно-технических, правоохранительных, экономических мер обеспечения национальной безопасности в информационной сфере. В свою очередь, именно через развитие этой сферы главным образом обеспечивается и ее безопасность [3].

Так, например, законодательно определен порядок технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам (приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» [4]), в целях обеспечения защиты государственных и общественных интересов, прав и законных интересов граждан деятельность по технической и (или) криптографической защите информации подлежит лицензированию (Указ Президента Республики Беларусь от 1 сентября 2010 г. № 450 «О лицензировании отдельных видов деятельности» [5]) и др.

Информационная безопасность сегодня является ключевым аспектом в обеспечении эффективной работы любой организации вне зависимости от формы собственности. В этой связи требования к квалификации IT-специалистов, занимающихся вопросами защиты информационных технологий, постоянно повышаются. Любые материальные вложения в аппа-

ратные и программные средства защиты информации будут малоэффективными или даже бессмысленными, если их будут обслуживать неквалифицированные специалисты.

Проблема сохранности конфиденциальной информации и коммерческой тайны существовала и ранее, но по мере развития электронных средств обработки и хранения данных повышается вероятность их утечки и незаконного копирования. В этой связи представляется весьма важным, чтобы ответственные за обеспечение информационной безопасности лица были соответствующим образом подготовлены к предотвращению несанкционированного доступа к внутренней инфраструктуре, незаконного завладения конфиденциальной информации и внесения изменений в базы данных.

Обеспечение информационной безопасности становится все более актуальным и в связи с тем, что информационный ресурс существенно влияет на распределение сил в конкурентной борьбе как на внутреннем, так и на международном рынках. Очевидно, что в целях информированности и координирования общих усилий в сфере защиты информационных ресурсов государства необходимо организовать проведение регулярных семинаров по текущим проблемам информационной безопасности, а также осуществлять постоянное повышение квалификации IT-специалистов в сфере технической и криптографической защиты информации.

Одной из причин необходимости регулярного повышения квалификации является быстрое устаревание актуальных знаний. Так, программные продукты крупнейших компаний претерпевают значительные изменения в среднем каждые два-четыре года, что требует регулярного отслеживания за обновлениями программ и отдельных модулей. Технические изменения же происходят еще быстрее. Разумеется, основы создания архитектуры информационных систем меняются гораздо медленнее и эти знания устаревают не так быстро, но для эффективной работы в данном направлении в любом случае требуется регулярное обновление имеющихся знаний.

Основной проблемой является малое количество действительно полезных для дальнейшего развития курсов в области информационной безопасности, поскольку многие из них подготовлены с использованием формального подхода и по большей части преследуют цель получения прибыли, а не реального повышения квалификации IT-специалистов.

В этой связи, признавая критическую важность кадрового потенциала в обеспечении информационной безопасности, по инициативе Оперативно-аналитического центра при Президенте Республики Беларусь и при активной поддержке Министерства образования весной 2020 года республиканское унитарное предприятие «Национальный центр обмена трафиком» (далее – РУП «НЦОТ») открыло новое направление деятельности – предоставление образовательных услуг.

Постановлением Министерства образования Республики Беларусь от 16 января 2020 года № 2 «О предоставлении права реализации образовательной программы повышения квалификации руководящих работников и специалистов» РУП «НЦОТ» предоставлено право реализации образовательной программы повышения квалификации руководящих работников и специалистов [6].

Указанная программа обучения ориентирована на повышение квалификации работников организаций и предприятий всех форм собственности, в обязанности которых входит обеспечение информационной безопасности, в частности решение вопросов технической и (или) криптографической защиты информации. Обучение прямо направлено на совершенствование компетенций, необходимых для осуществления деятельности в сфере информационной безопасности и (или) повышение профессионального уровня руководителей и специалистов, в том числе в области технической и (или) криптографической защиты информации.

Курсы повышения квалификации проводятся на основании постановления Совета Министров Республики Беларусь от 3 апреля 2020 года № 204 «О повышении квалификации по вопросам технической и (или) криптографической защиты информации» [7].

На сегодняшний день разработано 12 образовательных программ, целью которых стала передача слушателям современных теоретических знаний и практических навыков в области защиты информации. Очевидно, что данное направление показало свою актуальность и востребованность.

РУП «НЦОТ» во взаимодействии с профессиональными лекторами учреждений образования Республики Беларусь постоянно ведутся работы над совершенствованием образовательного процесса, внедрением востребованных техник и методик преподавания: деловые игры, дискуссии, обучение через погружение в реальные проблемные ситуации и др. В рамках реализации образовательной деятельности РУП «НЦОТ» активно развивает партнерскую сеть. Представители ведущих компаний –производителей программных и программно-аппаратных средств в области защиты информации уже выразили готовность к сотрудничеству. В настоящее время осуществляется процесс получения статуса авторизованного учебного центра известных во всем мире производителей программных решений, что позволит слушателям получать актуальные знания по продуктам в сфере защиты информации, а также подтверждать свои компетенции, не покидая пределов страны.

В 2021 году запланировано открытие двух новых программ: «Электронное правительство» и «Защита персональных данных», что более чем оправдано. Современное информационное общество ждет от государства простого, комфортного, быстрого и эффективного взаимодействия с гражданами и бизнесом. Такое взаимодействие может обеспечить электронное правительство – система государственного управления, основанная на автоматизации управленческих процессов в масштабах страны. Другими словами, под электронным правительством подразумевается совокупность информационно-коммуникационных технологий, которые обеспечивают взаимодействие граждан, бизнеса, различных ветвей государственной власти и чиновников при оказании государственных услуг. К слову, современный уровень развития белорусского е-правительства позволил Республике Беларусь войти в число 40 стран с индексом готовности к электронному правительству в 2020 году, согласно проводимому раз в два года исследованию ООН «E-Government Survey 2020: digital government in the decade of action for Sustainable development» [8].

Кроме того, в скором времени ожидается принятие Закона Республике Беларусь «О защите персональных данных» – первого в нашей стране нормативного правового акта, который бы комплексно регламентировал защиту прав и свобод граждан при сборе, обработке, распространении или предоставлении их персональных данных. Законопроект предусматривает создание уполномоченного органа, который будет принимать меры по защите прав субъектов персональных данных при обработке персональных данных.

Таким образом, Республика Беларусь, признавая что меры по обеспечению информационной безопасности должны совершенствоваться постоянно, независимо от роли IT-инфраструктуры в производственных процессах организации, определила, что собственники (владельцы) информационных систем и владельцы критически важных объектов информатизации, юридические лица, выполняющие работы и (или) оказывающие услуги в сфере информационно-коммуникационных технологий (перечень которых установлен в законодательстве), организуют на базе РУП «НЦОТ» не реже одного раза в три года повышение квалификации своих работников и (или) иных лиц, в обязанности которых входит обеспечение информационной безопасности по вопросам технической и (или) криптографической защиты информации. Только такой подход способен сократить количество несанкционированных доступов к внутренним инфраструктурам и свести к минимуму утечку данных, а не бороться с наступившими последствиями.

Вместе с тем, успех в области информационной безопасности может принести только комплексный подход, сочетающий как государственный (актуализация законодательства и контроль со стороны государства за уровнем информационной безопасности), так и административный (надлежащее руководство на уровне любой организации), а также программно-технический уровни (использование современного программного обеспечения и информационных технологий).

Список литературы

1. Википедия [Электронный ресурс]. – Режим доступа : https://ru.wikipedia.org/wiki/Ротшильд,_Натан_Майер. – Дата доступа : 12.04.2021.

2. Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс] : Указ Президента Респ. Беларусь, 9 ноя. 2010 г., № 575 : в ред. Указа Президента Респ. Беларусь от 24.01.2014 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2021.

3. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета Безопасности Респ. Беларусь, 18 мар. 2019 г., № 1 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

4. О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 [Электронный ресурс] : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 20 фев. 2020 г., № 66 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

5. О лицензировании отдельных видов деятельности [Электронный ресурс] : Указ Президента Респ. Беларусь, 1 сент. 2010 г., № 450 : в ред. Указов Президента Респ. Беларусь от 16.11.2020 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2021.

6. О предоставлении права реализации образовательной программы повышения квалификации руководящих работников и специалистов [Электронный ресурс] : постановление Министерства образования Респ. Беларусь, 16 янв. 2020 г., № 2 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2021.

7. О повышении квалификации по вопросам технической и (или) криптографической защиты информации [Электронный ресурс] : постановление Совета Министров Респ. Беларусь, 3 апр. 2020 г., № 204 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2021.

8. E-Government Survey 2020: digital government in the decade of action for Sustainable development [Electronic resourse]. – New York : Department of Economic and Social Affairs, 2020. – Mode of access : https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%0Survey%20(Full%20Report).pdf. – Date of access : 12.04.2021.

ЗАСЕДАНИЕ № 4
ВОПРОСЫ СТАНДАРТИЗАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 004.056

ОЦЕНКА ЗАЩИЩЕННОСТИ ПРОМЫШЛЕННЫХ СИСТЕМ УПРАВЛЕНИЯ

И.И. ЛИВШИЦ
Университет ИТМО г. Санкт-Петербург, Российская Федерация

Введение. Для обеспечения безопасности промышленных систем известно несколько методических подходов. Наибольшее внимание получили два кардинально различающихся подхода: предложение реализации дополнительных мер защиты информации, без изменения ИТ-инфраструктуры и создание новой концепции тотальной изоляции (например, архитектуры Zero Trust). Как отмечается многими компаниями в России и в мире, эти методические подходы не приводят к улучшению стабильности и безопасности промышленных систем.

Проблема обеспечения безопасности появилась еще в XX веке и в настоящий момент наиболее очевидным является подход «от функциональности». Этот подход заключается в том, что формирование и решение проблемы начинается в тот момент, когда производитель создает решение по спецификации, состоящей из требований функциональной безопасности, и далее проводит оценку по требованиям доверия. Для общего процесса обеспечения безопасности промышленных систем характерно то, что до настоящего времени в отрасли еще не сложилась целостная культура потребления безопасных ИТ-компонент, имеющих доказательства безопасности, проверяемые до необходимого уровня.

Только несколько поставщиков готовы предложить компоненты, имеющие доказанный уровень обеспечения безопасности Safety Integrity Level в соответствии с требованиями IEC серии 61508 и/или 61511. В работе рассмотрена проблема обеспечения безопасности промышленных систем с учетом ограничений: ресурсов, быстродействия, качества управления, методов подтверждения соответствия, формирования оценок остаточных рисков.

1. Требования к обеспечению безопасности промышленных систем. Проблема обеспечения безопасности для промышленных систем различного назначения (Industrial Control System, ICS) имеет давнее происхождение. Первые работы в данной области появились еще в XX веке при возникновении промышленных систем управления сложными техническими объектами. К особенностям предшествующих периодов можно отнести важное архитектурное обстоятельство – для зарубежных и отечественных центров экспертиз в данной области не существовало раздельного определения сущностей информационных технологий (ИТ) и информационной безопасности (ИБ). В связи с этим системы проектировались, создавались, проходили испытания и эксплуатировались как единое целое [1, 2].

Ранее основными требованиями были: обеспечение реализации заложенного функционала и устойчивая работоспособность программных (программно-аппаратных) комплексов [3–5]. Позже появились и законодательные инициативы, призванные упорядочить значительное количество отраслевых и регуляторных документов. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ и ряд подзаконных актов определили угрозы и меры защиты для обеспечения защищенности объектов критической информационной инфраструктуры (КИИ).

В стандартах IEC серии 61508 и/или 61511 показаны требования к функциональной безопасности, а методы обработки рисков содержатся в ISO 31000, IEC 31010 или ISO/IEC 27005. Важным преимуществом методики в системе ISO следует признать установленные ограничения, в частности, по времени, глубине экспертизы, точности результатов и пр. Опи-

сание требований функциональной безопасности, изложенных в стандартах ISO, даны в [6, 7], а IEC серии 61508 и/или 61511 в [8, 9] соответственно.

2. Оценка безопасности встроенных мер защиты. Известно о российском проекте по испытаниям PT Industrial Security Incident Manager и ProfiDIODE компании Oreol Security. Испытания включали проверку корректной работы и целостности данных в получаемой копии трафика, среда тестирования ограничена 100 Мбит/с, что соответствует стандартному значению в реальных ICS. Показано, что база экспертизы PT Industrial Security Threats Indicators превышает 4 тыс. правил, в том числе для выявления рисков в технологических сетях и поиска уязвимостей, которые эксплуатируются вредоносным программным обеспечением (ПО), например, Trisis, Triton. Несмотря на данные предложения, для оценки безопасности встроенных мер защиты необходимо определить состав функций, помимо базовых требований подсистемы аварийной защиты, например, в соответствии с IEC серии 61508 и/или 61511. Следует также заметить, что необходим серьезный анализ и достаточность быстродействия для анализа трафика, циркулирующего в реальных ICS.

В отчете Positive Technology показаны неутешительные результаты тестирования промышленных сетей, что позволило выявить узлы, на которых раскрывается важная информация (например, содержимое конфигурационных файлов). Показано, что причина многих инцидентов кроется в небезопасной конфигурации служб, и выявлены известные уязвимости, начиная с 2013–2014 гг. Нотация уязвимостей приводится в соответствии с принятой системой CVE (Common Vulnerabilities and Exposures) для общеизвестных уязвимостей ИБ.

3. Проблемы оценки доверия ИТ-компонент. В международных публикациях показана высокая доля рисков безопасности ICS в исходном коде ИТ-компонент [4]. Необходимо отметить, что применение «наложенных» СЗИ вносит свои риски, поскольку они также содержат множество уязвимостей, и, в том числе потенциально недоверенный исходный код. Применительно к нормативному регулированию отметим, что в РФ принят ГОСТ Р 57580.1-20175, в котором определена мера ЖЦ.8 по оценке прикладного ПО в соответствии с оценочным уровнем доверия ОУД 4. Кроме указанного ГОСТ Р, можно рекомендовать и иные НМД, специально посвященные оценке доверия, в частности: X.1254/ISO 29115 «Information Technology. Security techniques. Entity authentication assurance framework», в которых упомянуты спецификации уровней доверия к аутентификации: LoA1 – LoA4. Отметим также известные требования по аутентификации: ISO 29115:20136 и ISO/IEC 10181-2:19967. В РФ принят ГОСТ Р 54581–20118, которые определяет требования к оценке уверенности (confidence), как «убежденность в том, что оцениваемый объект будет функционировать в соответствии с заданным или установленным порядком» (пп. 2.4, 10, 11). Опубликован новый реестр инцидентов КИИ Critical Infrastructures Ransomware Attacks, в котором представлены публичные данные, в том числе раскрытые в официальных уведомлениях по безопасности. По частоте упоминания лидирует вредоносное ПО Maze, далее WannaCry, NetWalker, CryptoLocker и пр.

Для данной работы важно, что по области охвата лидируют правительственные учреждения, среди которых службы реагирования на чрезвычайные ситуации, далее – производственные объекты, транспортные системы, финансовые сервисы. Общая динамика роста инцидентов КИИ весьма тревожная: в 2018 г. раскрыто 68 инцидентов, в 2019 г. – 209 инцидентов (+ 207 %), за первое полугодие 2020 г. уже – 209 инцидентов. Не всегда и не все технические решения можно протестировать, и заранее определить векторы атак, и выявить критические уязвимости. Например, компания Industrial Defenica в рамках эксперимента для изучения угроз ICS развернула сеть Honeypot, принявшую на себя десятки тысяч атак. Важно, что Honeypot весьма эффективна в поиске 0-day уязвимостей и анализе «целевых» атак, но именно для «реалистичного» представления объектов КИИ могут быть сложности, например, IP-адреса в облачной платформе не будут выглядеть правдоподобно.

При формировании оценки доверия ИТ-компонент важно использовать базовый уровень обеспечения функциональной безопасности в ICS по факту создания, иначе говоря «as is». В некоторых публикациях, рассмотренных автором, показано, что поставщики СЗИ

полагают все ИТ-компоненты (контроллеры, инженерные станции и пр.) изначально абсолютно незащищенными перед любыми угрозами, и рекламируемые «наложенные» СЗИ просто необходимы. Более того, все рекламные публикации (даже на научно-практических на форумах «SOC», «ИБ КВО АСУТП», «КЗИ» и пр.), не содержат технических выкладок, сопровождающих технический анализ: достаточное быстродействие, потребляемая память, пропускная способность и пр. Очевидно, что если компоненты ПЛК проходят жесткое тестирование на соответствие известным требованиям IEC серии 61508 и/или 61511 и обладают доказанной реализацией заданного множества функциональной безопасности, то к «наложенным» СЗИ таких требований не предъявляется и, соответственно, они не проверяются. Подобное упущение может привести к серьезным нарушениям «сплошного» равнопрочного поля функциональной безопасности в целом для ICS.

С учетом иерархии управления в ICS очевидно, что для каждого уровня должны быть явно определены свои требования, и чем ниже уровень, тем более жесткие должны быть требования к обеспечению функциональной безопасности. Соответственно, вопрос применения «наложенных» СЗИ, способных обеспечить информационный обмен (прием информации с датчиков, анализ и выдача управляющего воздействия) с гарантированным откликом в установленное нормативное время (секунды и менее для уровня PLC и ниже) вызывает серьезные сомнения, поскольку является областью неопределенности и значимого риска. Дополнительно учтем требования IEC серии 61508 и/или 61511, согласно которым все пространства состояний (возможные сочетания открытых клапанов, вентилей, положений манипуляторов и пр.), а также переходы между ними, должны быть заранее определены и многократно протестированы на уровне всех ИТ-компонент ICS. В обязательном случае реализуется контур безопасности подсистемы аварийной защиты, который, уместно напомнить, является обязательной и неотъемлемой частью любой ICS.

Вызывает серьезное сомнение способность «наложенных» СЗИ «выдать» в канал управления верное управляющее воздействие, согласующееся с реакцией встроенной подсистемы аварийной защиты. В наилучшем случае «наложенное» СЗИ успевает не позже подсистемы аварийной защиты, но возникает не менее важная следующая проблема арбитража между логикой управления подсистемы аварийной защиты (зачастую является коммерческой тайной каждого производителя) и логикой СЗИ, также не являющейся публично доступной.

Заключение

1. В работе предложен обзор существующих подходов для решения проблемы обеспечения безопасности промышленных систем. Приняты во внимание доступные источники, как мировых, так и российских центров экспертизы, в том числе и ведущих поставщиков СЗИ. Отмечается, что формирование и решение указанной проблемы актуально и требует комплексного учета многих факторов: устаревшего подхода моделей угроз, игнорирования национальных ГОСТ Р/ГОСТ РВ и риск-ориентированных стандартов ISO, попыток раздельного анализа ИТ-компонент и решений ИБ.

2. Необходимо проблему обеспечения безопасности промышленных систем рассматривать в технических аспектах: требуемых ресурсов, заданного быстродействия, качества управления, методов подтверждения соответствия, формирования оценок остаточных рисков и иных исчислимых оценок. Требуется уделять первостепенное внимание развитию подхода «от функциональности», при котором обобщенно формирование и решение проблемы начинается в тот момент, когда производитель создает решение по спецификации, состоящей из требований функциональной безопасности, и далее проводит оценку по установленным и известным требованиям доверия.

3. Для решения проблемы обеспечения безопасности промышленных систем больше внимания следует уделять поставке ИТ-компонент, безопасных изначально и прошедших объективную и полную оценку соответствия функций безопасности в аккредитованных лабораториях в соответствии с требованиями применимых международных и национальных стандартов. Также необходимо и более широкое привлечение специализированных научных организаций и поставщиков ИТ-компонент.

Список литературы

1. Баранов, С. Н. Модели рисков в программных проектах / С. Н. Баранов [и др.] // Перспективные направления развития отечественных информационных технологий : мат-лы II Межрегиональной науч.-практ. конф. – Севастополь : Севастопольский гос. ун-т, 2016. – С. 45–46.

2. Соколов, Б. В. Имитационное моделирование живучести критических инфраструктур / Б. В. Соколов [и др.] // VII всеросс. науч.-практ. конф. «Имитационное моделирование. Теория и практика» (ИММОД-2015) : труды конференции в 2 т. Т. 1. – М. : Институт проблем управления им. В.А. Трапезникова РАН, 2015. – С. 162–167.

3. Верзилин, Д. Н. Неокибернетика: состояние исследований и перспективы развития / Д. Н. Верзилин, Б. В. Соколов, Р.М. Юсупов // Системный анализ в проектировании и управлении : сб. науч. тр. XXIII Междунар. науч.-практ. конф. – СПб. : Санкт-Петербургский политехн. ун-т Петра Великого, 2019. – С. 81–98.

4. Maggi, F. Attacks on Smart Manufacturing Systems: A Forward-looking Security Analysis [Электронный ресурс] / F. Maggi, M. Pogliani. – Режим доступа : https://documents.trendmicro.com/assets/white_papers/wp-attackson-smart-manufacturing-systems.pdf. – Дата доступа : 14.04.2021.

5. Claroty Biannual ICS Risk & Vulnerability Report: 1H 2020 [Электронный ресурс]. – Режим доступа : https://f.hubspotusercontent20.net/hubfs/2553528/Claroty_Biannual_ICS_Risk_Vulnerability_Report_1H2020.pdf. – Дата доступа : 14.04.2021.

6. Livshitz, I. I. IT security evaluation – «hybrid» approach and risk of its implementation / I. I. Livshitz, A. V. Neklyudov, P. A. Lontsikh // Journal of Physics: Conference Series. – 2018. – V. 1015, № 4. – P. 042030.

7. Лившиц, И. И. Методика оптимизации программы аудитов информационной безопасности / И. И. Лившиц, А. В. Неклюдов // Комплексная защита информации : мат-лы XXII науч.-практ. конф. – Новополоцк : Полоцкий гос. ун-т, 2017. – С. 135–139.

8. Лившиц, И. И. Метод оценивания безопасности облачных ИТ-компонент по критериям существующих стандартов / И. И. Лившиц // Труды СПИИРАН. – 2020. – Т. 19, № 2. – С. 383–411.

9. Лившиц, И. И. Практика управления киберрисками в нефтегазовых проектах компаний холдингового типа / И. И. Лившиц // Вопросы кибер безопасности. – 2020. – № 1 (35). – С. 42–51.

УДК 004:34

СОВЕРШЕНСТВОВАНИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д.Н. ЛАХТИКОВ
Учреждение образования «Академия Министерства внутренних дел Республики Беларусь», г. Минск, Республика Беларусь

В связи с развитием информационных технологий и их активным внедрением в различные сферы общества информационная безопасность становится одним из ключевых направлений деятельности и актуальным аспектом в сфере правового регулирования. При этом она выходит за пределы потребностей отдельных граждан или юридических лиц и трансформируется в одно из направлений развития государства на стратегическом уровне.

Развитие киберпространства и активное внедрение информационных технологий, например, на принципе распределенного (децентрализованного) реестра привело к созданию принципиально нового правового инструментария: умные контракты, электронно-цифровые подписи и др. [1, с. 45]. Возрастание роли информационной безопасности также связано и с появлением новых видов правонарушений в информационной сфере. Так, например, в интернет-банкинге – различные виды хищений денежных средств, в том числе с использованием вредоносного программного обеспечения. Все более распространенными становятся такие явления, как киберсквоттинг (захват доменных имен), т. е. регистрация доменного имени, частично сходного с уже зарегистрированным, или тождественного по написанию с иным средством индивидуализации (товарным знакам); брэндсквотинг – регистрация на определенной территории товарного знака, ранее не зарегистрированного, с целью продажи его заинтересованным лицам [1, с. 46]. При этом на первый план выходят вопросы защиты информации и кибербезопасности. При этом научная разработка проблем кибербезопасности и защиты информации проводились фрагментарно, комплексные исследования в этой области отсутствуют, зарубежом данной проблеме уделялось большее внимания.

В свою очередь в научной литературе отмечается, что процессы информатизации (цифровизации) в каком-то смысле «подчиняют» себе правовую материю, мотивируя правоприменителя к более гибкому толкованию правовых норм, с тем, чтобы обеспечить их действие в цифровой среде [2, с. 76].

В Республике Беларусь и во многих других странах имеется законодательство, регулирующее отношения в этой сфере, это преимущественно акты законодательства различного уровня и институциональной принадлежности. Например, Закон Республики Беларусь Закон Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации», Указы Президента Республики Беларусь № 60 от 01.02.2010 «О мерах по совершенствованию использования национального сегмента сети Интернет», № 196 от 16.04.2013 «О некоторых мерах по совершенствованию защиты информации», а также иными актами независимого регулятора в этой сфере.

В отдельных государствах принимаются законы о кибербезопасности, включая защиту информации (например, Латвия, Эстония и др.). Например, в Украине принят Закон от 05.10.2017 № 2163-VIII «Об основных принципах обеспечения кибербезопасности Украины», определяющий правовые основы обеспечения защиты интересов гражданина, общества и государства, национальных интересов в киберпространстве, государственную политику в сфере кибербезопасности и др. В рамках Европейского союза 17.04.2019 принят Регламент о кибербезопасности (526/2013), определяющий правовые основы кибербезопасности информационных и коммуникационных технологий, а также правовой статус Агентства Европейского союза по кибербезопасности.

Термин «безопасность» – это правовая категория, определяется как урегулированное правом состояние защищенности законных интересов личности, общества, государства при котором отсутствуют угрозы безопасности. Ключевым в определениях безопасности являет-

ся защищенность, что предполагает наличие качественной правовой системы в целом, а не ее отдельных элементов [3, с. 58]. С учетом повышения роли кибербезопасности и защиты информации, прежде всего в электронном виде, представляется целесообразной консолидация регулирования указанных вопросов.

В научной литературе выделяется несколько подходов правового регулирования кибербезопасности и защиты информации. Первый –заключается в том, что в различных законах урегулированы общие вопросы защиты информации и кибербезопасности. В нормативных актах другого уровня (например, Оперативно-аналитического центра при Президенте Республики Беларусь) без принятия дополнительных законодательных актов регламентируются частные вопросы этой сферы. Второй подход заключается в разработке отдельного закона, регулирующего общественные отношения в этой сфере.

Необходимо учитывать, что интерес государственных структур заключается в установлении правового регулирования в целях предотвращения угроз личной, государственной и общественной безопасности; представителей же информационного сообщества и многих пользователей интересует сохранение саморегулирования, основанного на этических нормах. В контексте сохранения регулирующей роли права, обеспечения баланса интересов целесообразно государственное вмешательство в регулирование общественных отношений в этой сфере в случаях, когда саморегулируемые организации, этические нормы оказались не в состоянии разрешить ситуации, негативные последствия которых стали повторяться, распространяться и затрагивать интересы значительного круга лиц [3, с. 59].

В свою очередь, касаясь разработки отдельного закона по вопросам кибербезопасности и защиты информации, целесообразной является реализация подхода, предусматривающего в отдельном законе урегулировать отношения, касающиеся кибербезопасности и защиты информации, при этом предусмотреть положения: основные принципы обеспечения кибербезопасности и защиты информации; систему обеспечения кибербезопасности (построение, функционирование); требования к защите информации; полномочия государственных органов, предприятий, учреждений, организаций, и граждан в этой сфере; требованиях к защите информации; критически важные объекты информатизации; безопасности Интернета; субъекты осуществляющие координацию и контроль в этой сфере.

Кибербезопасность и защита информации (представленной в электронном виде) в настоящее время является быстроразвивающейся сферой, требующей четкого определения правовых и организационных основы обеспечения ее эффективного функционирования. Принятие самостоятельного закона позволит комплексно урегулировать данную сферу отношений.

Таким образом, процесс информатизации продолжает активно развиваться, обусловливая технологические нововведения, актуализирующие проблемы правового характера в этой сфере. Все большую значимость приобретают вопросы обеспечение сохранности государственной и служебной тайны; информации, ограниченной для распространения, в информационно-коммуникационной среде. Решением этой задачи может стать создание более эффективной модели правового регулирования, которая могла гарантировать безопасность. В частности, целесообразно сосредоточить нормы, касающиеся кибербезопасности и защиты информации в одном законе. При этом необходимо помнить, что со временем понятие содержания безопасности может меняться, в частности объекты, подлежащие защите и субъекты ее осуществляющие.

Список литературы

1. Карцхия, А. А. Информационная безопасность: правовые аспекты / А. А. Карцхия, В. Л. Севостьянов // Правовая информатика. – 2018. – № 4. –С. 43–49.

2. Пучков, О. А. Новые угрозы кибербезопасности интернет-пространства и возможные правовые способы их предотвращения / О. А. Пучков // Правовое государство: теория и практика. – № 4 (62), ч. 1. – 2020. – С. 76–87.

3. Примак, Т. К. Цифровая безопасность: правовое регулирование, соотношение с кибербезопасностью / Т. К. Примак, О. А. Серова // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. – 2019. – № 2 (56). – С. 57–60.

УДК 004:34

О МЕЖДУНАРОДНОМ ДОГОВОРЕ О ПОРЯДКЕ ВЗАИМНОГО ПРИЗНАНИЯ ЭЛЕКТРОННЫХ ПОДПИСЕЙ

С.А. КИРЮШКИН
ООО Газинформсервис, Российская Федерация

Для обеспечения безбумажной трансграничной торговли, эффективность которой неоднократно доказана в различных международных форматах, требуется решить задачу взаимного признания странами-участницами электронной подписи, так как она имеет множество национальных особенностей.

Эта задача решается на различных международных площадках, прежде всего ЕАЭС, различные форматы ООН, в рамках союзного государства России и Беларуси и др.

В 2020–2021 году между Российской Федерацией и Республикой Беларусь был поведен первый этап пилотного проект по обмену электронными товаросопроводительными документами при трансграничной торговле между хозяйствующими субъектами с применением механизма Доверенной третьей стороны для обеспечения взаимного признания ЭЦП.

Координировали данный трансграничный проект Федеральная налоговая служба Российской Федерации и Министерство по налогам и сборам Республики Беларусь.

По итогам проведенного пилотного проекта можно констатировать, что на текущий момент сформировалась технологическая и организационная инфраструктура, а также все предпосылки для нормативно правового обеспечения решения задачи признания электронной цифровой подписи в электронном документе и обеспечения юридической силы электронных документов при трансграничном информационном взаимодействии бизнеса.

Согласно поправкам в Федеральный закон от 6.04.2011 № 63-ФЗ «Об электронной подписи», вступившим в силу в июле 2020 года (статья 7, часть 3): «Признание электронных подписей, созданных в соответствии с нормами права иностранного государства и международными стандартами, соответствующими признакам усиленной электронной подписи, и их применение в правоотношениях в соответствии с законодательством Российской Федерации осуществляются в случаях, установленных международными договорами Российской Федерации».

На сегодня создана технологическая и организационная основа для решения этой задачи, выполнен ряд пилотных проектов. Но, международного договора РФ, отвечающего требованиям части 3 статьи 7 63-ФЗ пока нет.

В случае успешной реализации такой международный договор может стать модельным и взят за основу для правового обеспечения взаимного признания трансграничной электронной подписи с другими странами и в рамках международных объединений с участием Российской Федерации.

В докладе рассмотрены некоторые взгляды на возможный проект международного договора, обеспечивающего указанные требования.

УДК 342.95

ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ: НЕКОТОРЫЕ АСПЕКТЫ СОВЕРШЕНСТВОВАНИЯ

М.В. ГУБИЧ
УО «Академия Министерства внутренних дел Республики Беларусь», г. Минск, Республика Беларусь

Введение. События последних десятилетий показали необходимость формирования и внедрения в юридическую практику средств, позволяющих осуществлять эффективное правовое воздействие на общественные отношения в условиях реализации кризисных обстоятельств, что является особенно актуальным для сферы обеспечения информационной безопасности объектов. В числе таковых, полагаем необходимым акцентировать внимание на специальных правовых режимах, содержащих в своем «арсенале» юридические средства, заранее адаптированные к конкретным кризисным обстоятельствам.

Среди нерешенных юридической наукой и практикой проблем обеспечения информационной безопасности можно указать на отсутствие единых подходов к пониманию сущности и содержания деятельности по информационному противодействию негативной информационной активности в сети Интернет, ее правовом режиме, субъектах, финансировании и оценке эффективности.

Позитивным видится определение перспективных областей применения механизмов государственно-частного партнерства в сфере обеспечения информационной безопасности и противодействия киберпреступности, преодоление проблем в правовом и организационном обеспечении данной формы взаимодействия.

1. Специальные правовые режимы. Абсолютное большинство нормативных правовых актов исходит из так называемых «обычных условий», в которых происходит разрешение различных вопросов в жизни гражданина, общества и государства. Исключение составляет законодательство о военном и чрезвычайном положении, основаниями введения которых являются исключительные обстоятельства. Вместе с тем на практике возникают определенные кризисные ситуации, при которых введение указанных положений не является обоснованным как с правовой, так и практической точек зрения, однако реагирование на изменившуюся ситуацию, используя законодательство «обычных условий», является достаточно затруднительным, особенно когда требуется принятие решительных и неотложных действий и мер, на согласование и утверждение которых, по общему правилу, необходимо продолжительное время и одобрение широкого числа заинтересованных государственных органов и должностных лиц. Иными словами, использование в определенных кризисных ситуациях стандартных процедур, установленных законодательством для «обычных условий», является не в полной мере оперативным и эффективным.

В этой связи видится весьма позитивным и своевременным подход Оперативно-аналитического центра при Президенте Республики Беларусь к решению задач в сфере обеспечения безопасности объектов информатизации, приказом которого от 20 февраля 2020 г. № 65 утверждены показатели уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах в случае создания угроз информационной безопасности либо в результате возникновения рисков информационной безопасности в отношении объекта информатизации. То есть указанным государственным органом осуществлена инициативная разработка критериев и их индикаторов, указывающих на наступление кризисной ситуации в сфере, являющейся «зоной ответственности» данного ведомства.

Следует акцентировать внимание на том, что в пункте 6 Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 содержится поручение организациям, эксплуатирующим объекты информатизации, обеспечить подготовку заключений на предмет соответ-

ствия данных объектов указанным выше показателям, а соответственно выработать управленческие, организационные и правовые механизмы осуществления деятельности при наступлении кризисных обстоятельств.

В ряду нормативных правовых актов, принятых в реализацию Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449, особое внимание заслуживает приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66, утвердивший ряд положений в сфере технической защиты информации, в том числе обрабатываемой на критически важных объектах информатизации. Позитивным видится построение системы обеспечения безопасности на основе функционального подхода – «обеспечение информационной безопасности критически важного объекта информатизации достигается путем выполнения совокупности правовых, организационных и технических мер, направленных на блокирование (нейтрализацию) угроз информационной безопасности критически важного объекта информатизации, реализация которых может привести к прекращению или нарушению функционирования этого объекта, обеспечиваемого (управляемого, контролируемого) им процесса, нарушению конфиденциальности, целостности, доступности обрабатываемой информации».

Выбор в качестве основы деятельности по обеспечению безопасности функционального подхода позволил предложить конкретный порядок осуществления деятельности по созданию и функционированию системы информационной безопасности критически важного объекта информатизации, что, по своей сути, является ярким примером реализации специального правового режима, как точечного инструмента повышения эффективности государственного регулирования. В этой связи полагаем возможным рассматривать принятие на государственном уровне сугубо прогностических нормативных правовых актов, связанных с разработкой алгоритмов функционирования государственных органов, организаций и иных субъектов инфраструктуры безопасности, в условиях возможной реализации угроз национальной безопасности, как сигнал, указывающий на готовность законодателя и государственных органов к принятию в арсенал новых правовых средств нелинейного регулирования правоотношений.

2. Информационное противодействие негативной информационной активности в сети Интернет. В настоящее время мировое сообщество, и Республика Беларусь не стала исключением, столкнулось с необходимостью осуществления противодействия негативной информационной активности в сети Интернет, в том числе вовлечению населения в общественно-опасную деятельность с использованием информационно-коммуникационных технологий (экстремистские группы, профашистские, неонацистские и националистические движения, фанатские сообщества, деструктивные религиозные объединения, псевдоисламский радикализм, суицидальные группы и т. д.).

До настоящего времени учеными, практиками и законодателем не выработаны единые подходы к пониманию сущности и содержания информационного противодействия вовлечению в общественно-опасную деятельность посредством сети Интернет, что приводит к использованию разной терминологии, неопределенности объемов осуществляемой деятельности, субъектов и объекта осуществляемой деятельности и т. д.

Неясен правовой режим осуществления информационного противодействия вовлечению в общественно-опасную деятельность посредством сети Интернет, что обусловлено специфическими мерами и методами противодействия, которые осуществляются с использованием специальных программно-аппаратных средств и, как правило, имеют технические способы реализации. Так, информационному противодействию вовлечению в общественно-опасную деятельность посредством сети Интернет одновременно присущи элементы профилактики, оперативно-розыскной деятельности и мониторинга массовой информации. Однако, рассматриваемая деятельность обладает рядом специфических свойств, отличающих ее от профилактики, оперативно-розыскной деятельности и мониторинга массовой информации по следующим причинам.

Для того чтобы осуществлять корректирующее воздействие на лицо в целях недопущения совершения правонарушений необходимо это лицо выявить. Вместе с тем, например, для того чтобы выявить конкретное лицо, являющееся участником экстремистской группы в социальной сети, необходимо осуществить ряд мероприятий, не являющихся по своей при-

роде профилактическими: провести мониторинг социальных сетей и иных ресурсов для идентификации конкретных лиц, их учетных записей, почтовых ящиков, при этом выделить среди найденных тех лиц, которые являются объектами корректирующего воздействия национальных субъектов профилактики правонарушений.

В этой связи представляется логичным рассматривать указанное в плоскости оперативно-розыскной деятельности, тем более национальное законодательство предусматривает проведение соответствующего оперативно-розыскного мероприятия – «контроль в сетях электросвязи». Однако данное оперативно-розыскное мероприятие в случае отсутствия сведений о персональных данных гражданина, в отношении которого предполагается проведение контроля в сетях электросвязи, до их установления проводится только «при наличии сведений об используемых гражданином абонентском номере, адресе электронной почты, уникальном коде идентификации, абонентском устройстве». Таким образом, применительно к рассматриваемому примеру, для проведения данного мероприятия отсутствуют правовые основания, так как из смысла статьи 31 Закона Республики Беларусь «Об оперативно-розыскной деятельности» субъекту оперативно-розыскной деятельности должны быть известны либо персональные данные лиц, вовлекаемых в общественно-опасную деятельность, либо их учетные записи в социальных сетях, почтовые ящики и т. п.

Информационное противодействие вовлечению в общественно-опасную деятельность посредством сети Интернет от мониторинга массовой информации отличают, в первую очередь, цели мониторинга, который проводится для оценки соблюдения законодательства о средствах массовой информации, а, во вторую, – отсутствие правоохранительных компетенций у республиканского органа государственного управления в сфере массовой информации, которым является Министерство информации Республики Беларусь.

Неразрешенным является вопрос о субъектах информационного противодействия. Изучение нормативных правовых актов, устанавливающих права, обязанности, цели и задачи функционирования государственных органов и организаций, являющихся субъектами профилактики правонарушений, и органов, осуществляющих оперативно-розыскную деятельность, показывает, что все они в той или иной степени, в зависимости от назначения, обладают компетенциями на осуществление противодействия вовлечению в общественно-опасную деятельность посредством сети Интернет. Однако, ни один из данных субъектов, исходя из анализа законодательства, не может быть признан ответственным за рассматриваемое направление деятельности.

Отдельным блоком проблем являются вопросы, связанные с финансированием рассматриваемой деятельности. Так, помимо наличия в штате организации необходимого количества сотрудников, видится необходимость привлечения специалистов, в обязанности которых будет входить как мониторинг сети Интернет, так и создание собственных интернет-ресурсов, наполнение их и иных информационных площадок печатными, аудио-, аудиовизуальными и другими информационными сообщения и материалами. Для создания такого контента необходимы специалисты в рекламной сфере, пиаре, оценке степени психологического и иного воздействия созданного контента, эксперты по продвижению интернет-ресурсов и распространяемого контента, художники, режиссеры видеороликов, постановщики, актеры и т. д., что влечет отдельный вопрос финансирования этой деятельности.

Полагаем необходимым подчеркнуть еще одну проблему, которую необходимо будет разрешить субъектам информационного противодействия, – как оценить эффективность такой деятельности.

3. Государственно-частное партнерство. В настоящее время в Республике Беларусь создана законодательная база государственно-частного партнерства, сформирована институциональная среда и реализуются первые пилотные проекты. Проанализировав содержание национальных нормативных правовых актов в данной сфере можно отметить, что: законодателем представлены необходимые правовые основания для осуществления государственно-частного партнерства в сфере обеспечения информационной безопасности и противодействия киберпреступности; данная форма сотрудничества признана наиболее эффективной моделью обеспечения информационной безопасности; основными целями рассматриваемой формы

взаимодействия являются привлечение квалифицированных кадров, технологий, капитала частных предприятий, повышение эффективности использования бюджетных средств; государство заинтересовано в развитии механизмов обеспечения информационной безопасности.

Органы внутренних дел при решении возложенных на них задач (особенно в сфере обеспечения задач информационной безопасности и противодействия киберпреступности) испытывают потребность в квалифицированных специалистах в области информационных технологий, в специальном программном обеспечении, дорогостоящих технических комплексах и т. п. В условиях государственного финансирования и имеющихся бюджетных ограничений удовлетворение указанных потребностей без привлечения дополнительных значительных финансовых инвестиций является затруднительным. Вместе с тем национальный сегмент коммерческих компаний, специализирующихся на вопросах оказания услуг в сфере обеспечения информационной безопасности, имеет определенный опыт и технические решения в областях обнаружения и противодействия вредоносным воздействиям на компьютерные системы и сети, анализа киберинцидентов и фиксации электронных доказательств. При этом данные организации не только показывают высокую эффективность, но и заинтересованы в расширении своей деятельности.

Представляется интересным отметить опыт Российской Федерации, в соответствии с Доктриной информационной безопасности которой к субъектам, являющимся участниками системы обеспечения информационной безопасности, отнесены собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации, организации денежно-кредитной, банковской и иных сфер финансового рынка, операторы связи и информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые участвуют в решении задач по обеспечению информационной безопасности.

В этой связи представляется обоснованным полагать, что такие коммерческие организации могут быть задействованы в деятельности по обеспечению информационной безопасности Республики Беларусь. Тем более что правовые основания для этого предоставлены Концепцией обеспечения национальной безопасности, в соответствии с которой граждане, общественные и иные организации наравне с государством отнесены к субъектам обеспечения национальной безопасности.

Вместе с тем до настоящего времени отсутствует информация о реализации в Республике Беларусь инфраструктурных проектов в рассматриваемой сфере. Представляется, что указанная ситуация обусловлена, в первую очередь, тем, что законодателем не была учтена специфика различных отраслей, в которых возможна реализация проектов государственно-частного партнерства, в том числе специфика осуществления правоохранительной деятельности в сегменте обеспечения информационной безопасности и противодействия киберпреступности.

Существенным проблемным аспектом в правовом регулировании государственно-частного партнерства является отсутствие в законодательстве положений, регламентирующих вопросы, связанные с созданием информационно-коммуникационной инфраструктуры, разработкой и внедрением информационных и телекоммуникационных технологий, посредством которых будут протекать информационные процессы с использованием сведений, образующихся в процессе осуществления правоохранительной деятельности, и иной информации, распространение которой ограничено. Разрешение данного проблемного аспекта является особенно значимым для практики государственно-частного партнерства в сфере обеспечения информационной безопасности и противодействия киберпреступности, по причинам циркуляции огромных объемов данных, содержащих охраняемую законом информацию, а также тяжести последствий, которые могут наступить в результате разглашения или утраты такой информации.

В этой связи отсутствие специального правового регулирования является существенным сдерживающим фактором, ограничивающим возможности развития механизмов госу-

дарственно-частного партнерства, востребованных как в целом в сфере обеспечения информационной безопасности, так и в таком ее сегменте как противодействие киберпреступности.

Заключение. В современных условиях гипердинамичности общественных отношений представляется необходимой разработка новых правовых средств и механизмов, позволяющих осуществлять более оперативное и эффективное реагирование на складывающие обстоятельства. В этой связи видится актуальным проведение исследований, направленных на разработку правовой основы специальных правовых режимов обеспечения информационной безопасности на основе функционального подхода, а также практических аспектов, необходимых для их реализации.

Первоочередными проблемами, подлежащими разрешению для осуществления эффективного информационного противодействия вовлечению в общественно-опасную деятельность посредством сети Интернет, являются разработка единых подходов к пониманию сущности и содержания рассматриваемой деятельности, определение ее правового режима, субъектов, источников финансирования и оценке эффективности.

Несмотря на то что в Республике Беларусь в целом создана правовая основа для решения задач обеспечения информационной безопасности в форме государственно-частного партнерства, имеются как правовые, так и организационные проблемы реализации таких проектов, в том числе связанные с отсутствием специальных норм, отражающих специфику осуществления правоохранительной деятельности в сегменте обеспечения информационной безопасности и противодействия киберпреступности.

УДК 004.056

МЕЖДУНАРОДНЫЙ ЮРИДИЧЕСКИ ЗНАЧИМЫЙ ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

Е.О. СОКОЛОВ
Gazprom International, г. Санкт-Петербург, Российская Федерация

Введение. Важность и актуальность применения современных ИТ не вызывает никаких сомнений, особенно если решение позволяет обеспечить одновременно несколько преимуществ для крупной компании. К таким преимуществам можно отнести, традиционно, вопросы экономической эффективности, технической реализации и функциональной полноты, обеспечения заданного уровня информационной безопасности. В полной мере к таким современным ИТ можно отнести технологии электронного документооборота (ЭДО). Определенно, в настоящее время на первое место обоснованно вышла проблема Compliance, обеспечения соответствия законодательным, регуляторным и иным применимым требованиям, что исключительно важно именно для ЭДО. Следует отметить, что в РФ и в мире реализуется множество проектов, как «чистого» ЭДО, построенных на известных ИТ-компонентах, так и проектах сложных коммерческих систем, ранее созданных для иных целей, например, EDI (Electronic Data Interchange, электронный обмен данными).

В представленной статье дается некоторый общий аналитический срез некоторых наиболее известных проектов, показаны основные современные тенденции. В развитие существующих подходов представлена новая схема обеспечения юридически значимого ЭДО, которая обладает рядом значительных преимуществ, построена на базе современных риск-ориентированных стандартов и прошла несколько успешных этапов практической апробации. Представленные результаты могут быть востребованы в российских и международных компаниях, для которых реализация защищенного и безопасного ЭДО является не данью моде «цифровизации», а насущной технологической необходимостью.

1. Известные проекты. В настоящее время многие крупные компании заявили о выполнении широкого спектра проектов «цифровой» трансформации, в том числе – проектов ЭДО. В частности, известны проекты Сбербанка, ПАО «Ростелеком», X5, «Газпром нефть» и некоторых других компаний. Важной импульс проектам «цифровой» трансформации придал эксперимент с переводом кадрового ЭДО в электронную форму. Эта инициатива получила законодательную поддержку – в апреле 2020 г. принят Федеральный закон «О проведении эксперимента по использованию электронных документов, связанных с работой» от 24.04.2020 № 122-ФЗ.

Следует обратить внимание на несколько ключевых аспектов известных проектов – значительный «зоопарк» систем, которые известные участники эксперимента применяют – от «классических» тяжелых ERP – SAP, Oracle и пр. до российских известных решений – 1С и «Галактика». Весьма интересно, что по некоторым данным, проекты на базе 1С занимают до 53 % рынка, когда на долю SAP и Oracle приходится только 22 % и 3 % соответственно. Кроме того, весьма интересно, что все рассмотренные выше участники эксперимента ориентируются на использование простой электронной подписи (ПЭП), данные которой загружают через шлюзы Единая система идентификации и аутентификации (ЕСИА). Вызывает определенную обеспокоенность способность всех участников «цифрового» эксперимента корректно запрашивать и проверять НЭП, без участия широко известных и доказавших свою эффективность сервисов безопасности, например, удостоверяющее центры (УЦ).

2. Оценка рисков известных проектов. На основании доступных материалов компаний – участников «цифрового» эксперимента и различных докладов (например, на 9-й практической конференции «Электронный документооборот», прошедшей 13–14 апреля в Москве), можно оценить основные риски:

1) Значительная сложность интеграции ИТ «зоопарка» – SAP, Oracle, Lotus Notes;

2) Многие пользователи не имеют возможности видеть маршруты движения документов;

3) Недостаточный уровень безопасности при проверке ПЭП на сайте Минтруда;

4) Многие представители жалуются, что нельзя подписывать документы «задним числом»;

5) Дублирование данных, которые закачивают через API в свои системы;

6) Слабый контроль работников, которые не приходят, не подписывают и увольняются;

7) Недостаточная судебная практика урегулирования «цифровых» исков.

С учетом данных рисков в компании Gazprom International предприняла определенные шаги на стадии проектирования с целью изучения, оценивания и минимизации воздействия негативных последствий на бизнес-процессы компании. Важной особенностью проекта ЭДО в компании Gazprom International является ориентация на современных стандартах ISO (ISO/IEC), прежде всего – «целевые» стандарты «риск-менеджмента» ISO 31000, IEC 31010 или ISO/IEC 27005. Кроме того, на всех этапах создания проекта ЭДО выполняется подробный аудит в области информационной безопасности.

3. Предложения по созданию международно значимого ЭДО. Проект международно значимого ЭДО был начат в Gazprom International в 2018 г. Первый этап затрагивал создание базовой ИТ-инфраструктуры на базе решений 1С, формирование подходом для обмена документами в защищенном режиме в различных юрисдикциях. Необходимо отметить, что результаты первого этапа были настолько успешны и важны, что проект был подан на 4-й международный конкурс партнерской сети «1С» и занял 1-е место в Центральной и Восточной Европе. Среди важных преимуществ необходимо отметить повышение организационной эффективности компании, которая по оценкам специалистов Gazprom International позволила в 4 раза сократить сроки согласования документов и различных управленческих решений, а также повысить исполнительскую дисциплину. Также важным конкурентным преимуществом является то, что рутинное управление бизнес-процессами дополнено функциями делегирования задач и замещения, а интерфейс и объекты конфигурации адаптированы для пользователей на английском и русском языках.

Вторым этапом проекта ЭДО, который стартовал в ноябре 2020 г., стала реализация полного цикла договорной работы в разных юрисдикциях. Далее в рамках 2-го этапа были автоматизированы бизнес-процессы согласования служебных записок, командировок и пр. Соответственно, по итогам 2-го этапа собственными силами был создан конкретный продукт корпоративного уровня, способный успешно решать различные задачи во всех локациях компании.

В настоящий момент рабочая группа выполняет 3-й этап работ, целью которого определено создание международного юридически значимого ЭДО. Этот этап предусматривает большой перечень отдельных важных работ, среди которых создание собственных УЦ, оперирование несколькими видами квалифицированных электронных подписей, поддержание собственной безопасной ИТ-инфраструктуры и безусловное соответствие применимому законодательству. Общая концептуальная схема 3-го этапа проекта ЭДО показана на рисунке 1.

Дадим некоторые пояснения – для направления юридически значимых документов сервер ЭДО взаимодействует с сервером оператора (например, «Диадок»), которые обеспечивает безусловно соответствие законодательству РФ при передаче документов в государственные органы исполнительной власти с заданным уровнем информационной безопасности. В этом процессе используется усиленная квалифицированная электронная подпись (УКЭП), выданная УЦ «СКБ-Контур», но допускается использование для ряда приложений неквалифицированной электронной подписи (НЭП). В процессе аналитических исследований было принято решение не использовать ПЭП и сервисы ЕСИА. «Цепочки доверия» показаны красным пунктиром, соответственно, обеспечивается прослеживаемость от УЦ (в различных юрисдикциях), до аккредитующих центров с соответствующими юридическими полномочиями.

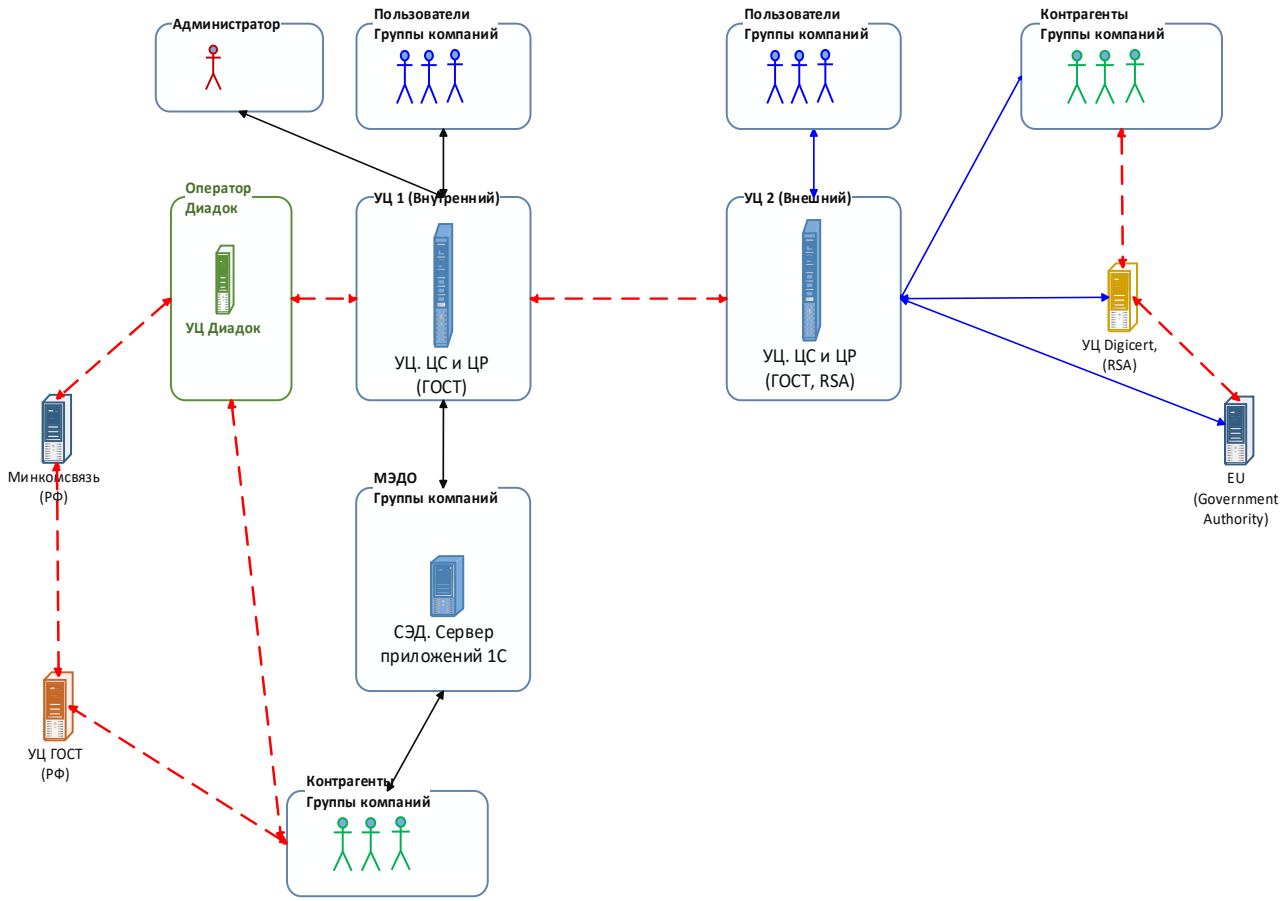


Рис. 1. Общая концептуальная схема 3-го этапа проекта ЭДО

4. Сценарии применения сервисов ЭДО. С учетом предложенной концептуальной схемы 3-го этапа проекта ЭДО предложены 3 возможных сценария применения сервисов ЭДО – только между контрагентами в России, между контрагентами в России и в мире и только между контрагентами в мире (табл. 1).

Таблица 1

Сценарии применения сервисов ЭДО

№	Локация контрагентов	Тип сертификата	Крипто-провайдер	Описание операции
1.	Россия / Россия	УКЭП	CryptoPro CSP	Подписание / шифрование документа; На карте FNC используется УКЭП (ГОСТ); Операции выполняются с бесконтактного считывателя ACR1252U, подключаемого к лэптопу работника компании; На лэптопе используется CryptoPro CSP; Провайдер МЭДО ведет проверку и протоколирование валидности УКЭП / УКЭП
2.	Россия / Мир или Мир / Россия	УКЭП / НЭП	CryptoPro CSP	Подписание / шифрование документа; Для обмена данными Компания Группы – Компания Группы: на карте FNC (в России) используется УКЭП, выданный аккредитованным УЦ в России (ГОСТ), на лэптопе используется CryptoPro CSP, а на карте FNC (в мире) используется НЭП, выданный аккредитованным УЦ в России (ГОСТ) и на лэптопе используется CryptoPro CSP; Операции выполняются с бесконтактного считывателя ACR1252U, подключаемого к лэптопу работников Компании Группы; Провайдер МЭДО ведет проверку валидности УКЭП / НЭП (CryptoPro CSP)

Окончание табл. 1

№	Локация контрагентов	Тип сертификата	Крипто-провайдер	Описание операции
3.	Мир / Мир	НЭП / НЭП	CryptoPro CSP / Microsoft CSP	Подписание / шифрование документа; Для обмена данными Компания Группы – контрагент: на карте FNC используется НЭП, выданный доверенным УЦ Компании (RSA, ECDSA). На лэптопе используется Microsoft CSP. У контрагента компании используется НЭП (RSA, ECDSA) и Microsoft CSP; Для обмена данными Компания Группы – Компания Группы: на карте FNC используется НЭП, выданный аккредитованным УЦ в России (ГОСТ). На лэптопе работников Компании Группы используется CryptoPro CSP; Операции выполняются с бесконтактного считывателя ACR1252U, подключаемого к лэптопу работника компании; Провайдер МЭДО ведет проверку валидности НЭП (только при CryptoPro CSP)

Заключение. В работе предложена новая схема обеспечения юридически значимого ЭДО, которая обладает рядом значительных преимуществ, прежде всего: современные риск-ориентированные стандарты, единая интеграционная платформа, равнопрочная система «цепочек доверий» УЦ и ориентация на УКЭП/НЭП. Кроме того, важно отметить, что все этапы проекта юридически значимого ЭДО прошли последовательно практическую апробацию. Представленные результаты могут быть востребованы в российских и международных компаниях, для которых реализация защищенного и безопасного ЭДО является не данью моде «цифровизации», а насущной технологической необходимостью.

Список литературы

1. Лившиц, И. И. Проектирование международного значимого электронного документооборота для компаний холдинового типа / И. И. Лившиц, Е. О. Соколов // Вопросы кибербезопасности. –2020. – № 5 (39). – С. 61–68.

2. Басырова, А. А. Анализ методики аудита информационной безопасности предприятия с помощью аутсорсинговых компаний / А. А. Басырова, И. И. Лившиц // Автоматизация в промышленности. – 2020. – № 7. – С. 6–9.

3. Брюховецкий, К. А. Анализ влияния регламента General Data Protection Regulation на деятельность предприятий топливно-энергетического комплекса / К. А. Брюховецкий, И. И. Лившиц // Энергобезопасность и энергосбережение. – 2020. – № 5. – С. 55–63.

4. Лившиц, И. И. Оценка степени влияния General Data Protection Regulation на безопасность предприятий в Российской Федерации / И. И. Лившиц // Вопросы кибербезопасности. – 2020. – № 4 (38). – С. 66–75.

УДК 034.096

ПРАВОВАЯ ОХРАНА ИЗОБРАЖЕНИЙ ГРАЖДАН В СЕТИ ИНТЕРНЕТ

Т.В. РАДЫНО
Республиканский союз промышленников и предпринимателей, г. Минск, Республика Беларусь

Общественные отношения в современном информационном обществе все в большей степени сопряжены с применением цифровых технологий. Возникновение новых правоотношений в цифровой сфере, адаптация традиционных правовых институтов к информационному цифровому пространству становятся объективной реальностью трансформации права. Глобальный характер цифровизации обусловливает признание необходимости принятия незамедлительных мер адаптации действующей системы права к процессам, происходящим в цифровом пространстве, выработке действенных правовых механизмов обеспечения защиты нематериальных благ человека, к которым относится и его непосредственное изображение.

Назрела острая необходимость своевременного законодательного регулирования новых общественных отношений, возникающих в связи с цифровизацией, внедрением новых механизмов реализации прав и свобод, обладающих виртуальным выражением. Для законодательного определения баланса между свободой личности в цифровом обществе и иными конституционно значимыми ценностями необходима правовая институционализация новых информационно-цифровых возможностей как личности, так и органов государственной власти. Особое значение в связи с развитием сети Интернет приобрела проблема правовой охраны изображения физического лица. Гражданин в связи с повсеместным размещением в киберпространстве изображений физических лиц – как с, так и без их согласия – должен иметь право на защиту сведений о своей личности всеми возможными правовыми способами.

Несмотря на то, что нарушение порядка опубликования фото-, видеоизображений в сети Интернет может повлечь как гражданско-правовую, так и административную и уголовную ответственность, распространение изображений физических лиц, изготовленных посредством различного рода фото- и видеосъемок, в средствах массовой информации (далее – СМИ), включая ресурсы глобальной компьютерной сети Интернет, с серьезным нарушением прав и законных интересов граждан имеет место.

Использование изображения гражданина без его согласия является вторжением в частную жизнь, а также нарушением права на личную тайну. Согласно Конституции Республики Беларусь, человек, его права, свободы и гарантии их реализации являются высшей ценностью общества и государства, обеспечение прав и свобод граждан Республики Беларусь – высшая цель государства; государство гарантирует охрану прав и свобод граждан Беларуси. Каждому гарантируется защита его личных неимущественных прав, таких как свобода и неприкосновенность личности, личная жизнь, честь и достоинство. К охраняемым нематериальным благам относится и внешний облик человека, принадлежащий ему от рождения, не отчуждаемый и не передаваемый иным способом, а также основанное на нем право на изображение гражданина.

Национальное законодательство воспроизводит принципы Всеобщей декларации прав человека, где предусмотрено, что никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию; каждый человек имеет право быть защищенным от такого вмешательства или таких посягательств. Согласно пункту 1 статьи 17 Международного пакта о гражданских и политических правах никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию. Право на уважение частной и семейной жизни закреплено также в статье 8 Конвенции о защите прав человека и основных свобод, официальная интерпретация положений которой содержится в решениях Европейского Суда по правам человека, причем «личная жизнь» – это широкое понятие, которое распространяется на множество аспектов самоидентификации человека, включая его имя и изображение.

Изображение человека представляет собой один из главных атрибутов его личности, поскольку оно демонстрирует уникальные характеристики человека и отличает его от всех остальных; право на защиту своего изображения является одним из важнейших элементов личностного развития и предполагает право контролировать использование данного изображения, в том числе право не разрешать его опубликование.

В связи с вышеизложенным, государство обязано принимать все доступные ему меры для создания правового порядка, необходимого для полного осуществления прав и свобод граждан Республики Беларусь, обеспечивать правовое регулирование, необходимое для полной реализации конституционных прав и свобод граждан и обеспечения своевременной и эффективной их защиты, включая выработку и закрепление действенного правового механизма использования и охраны изображения гражданина.

Конституционные нормы о гарантировании прав и свобод личности (часть первая статьи 2, часть третья статьи 21, часть первая статьи 25, статья 28 Конституции) находят развитие в пункте 2 статьи 1 Гражданского кодекса Республики Беларусь (далее – ГК): отношения, связанные с осуществлением и защитой неотчуждаемых прав и свобод человека и других нематериальных благ (личные неимущественные отношения, не связанные с имущественными), регулируются гражданским законодательством, поскольку иное не вытекает из существа этих отношений. Нематериальные блага защищаются в случаях и порядке, предусмотренных гражданским законодательством. Следовательно, именно гражданское законодательство определяет правовые механизмы осуществления и защиты нематериальных благ, в том числе внешнего облика гражданина как нематериального блага и права на изображение гражданина.

В то же время, законодательством Республики Беларусь, в отличие от Российской Федерации, право гражданина на собственное изображение прямо не отнесено к нематериальным благам, подлежащим защите в порядке, установленном гражданским законодательством. Приходится констатировать, что нормы о правовой охране изображения гражданина сегодня отсутствуют, право гражданина на охрану изображения текстуально не закреплено, несмотря на необходимость его легального признания. Тем не менее, внешний облик гражданина по своей сущностной характеристике очевидно относится к числу нематериальных благ, охраняемых Конституцией: как самодостаточное личное нематериальное благо, изображение гражданина представляет собой его внешний (индивидуальный) облик в объективированной форме, например, в произведении изобразительного искусства, на фотографии или видеозаписи в конкретный момент времени.

Такой подход согласуется со статьей 151 ГК («Нематериальные блага»), устанавливающей, что жизнь и здоровье, достоинство личности, личная неприкосновенность, честь и доброе имя, деловая репутация, неприкосновенность частной жизни, личная и семейная тайна, право свободного передвижения, выбора места пребывания и жительства, право на имя, иные личные неимущественные права и другие нематериальные блага, принадлежащие гражданину от рождения или в силу акта законодательства, неотчуждаемы и непередаваемы иным способом. Статья 151 ГК прямо не указывает на возможность обращения за судебной защитой и в случаях нарушения права гражданина на изображение, но и не исключает ее. Таким образом, хотя возможность правовой защиты нарушенного права гражданина на охрану его изображения имеет место, исходя из основных начал гражданского законодательства и применения аналогии закона, но она существенно затруднена.

Следует отметить, что в Гражданском кодексе Республики Беларусь 1964 года имела место статья 509 «Охрана интересов гражданина, изображенного в произведении изобразительного искусства», нормами которой было установлено, что распространение изображений лица допускается лишь с его согласия, а после его смерти – с согласия пережившего супруга и детей умершего. Исключение составляли случаи, когда изображение распространялось в государственных или общественных интересах, или изображенное лицо позировало автору за плату.

Таким образом, право на изображение гражданина как личное неимущественное право, являющееся нематериальным благом, должно быть обеспечено законными способами его осуществления и защиты, чтобы в случае посягательства на указанное благо (в том числе путем обнародования и распространения изображения гражданина без его согласия) была обеспечена возможность прибегнуть к разрешенным в статье 11 ГК способам защиты, среди

которых пресечение действий, нарушающих право или создающих угрозу его нарушения, самозащита права, компенсация морального вреда.

Отдельные вопросы защиты изображения регулируются нормами иных законодательных актов: согласно пункта 9 статьи 10 закона Республики Беларусь от 10.05.2007 № 225-З «О рекламе» по общему правилу не допускается использование образов граждан Республики Беларусь в рекламе без их согласия или согласия их законных представителей; в соответствии с пунктом 4 статьи 34 закона Республики Беларусь от 17.07.2008 № 427-З «О средствах массовой информации» предусмотрена обязанность журналиста СМИ получать согласие физических лиц на проведение видеозаписи, кино- и фотосъемок. Исключение составляют случаи проведения съемок в местах, открытых для массового посещения, на массовых мероприятиях, а также если приняты меры против возможной идентификации данного лица посторонними лицами, при условии, что распространение этих материалов не нарушает конституционных прав и свобод личности и необходимо для защиты общественных интересов.

Таким образом, нормы специальных законов обеспечивают лишь отдельные аспекты защиты образа и изображения физического лица. Вопрос охраны изображения гражданина, включая особенности обнародования и дальнейшего использования такого изображения, и конкретные способы охраны прав и законных интересов изображенного, требует дополнительной доктринальной проработки с учетом оценки правовых последствий.

30 октября 2018 г. прошло заседание Конституционного Суда Республики Беларусь, на котором установлено (решение № Р-1145/2018), что в действующем законодательном регулировании ***имеется правовой дефект***, обусловленный отсутствием в гражданском законодательстве надлежащего правового механизма использования и охраны изображения гражданина: отсутствуют прямые нормы, регламентирующие охрану изображения гражданина. По сути, Конституционный Суд констатировал наличие правовой неопределенности в гражданском законодательстве в части регулирования общественных отношений, связанных с надлежащими использованием и охраной изображения гражданина, в связи с чем нарушаются права граждан, изображенных на фото- или видеозаписи без их воли или согласия, закрепленные в статьях 28 и 59 Конституции.

Очевидно, что включение в ГК норм, определяющих особенности охраны изображения гражданина, является целесообразным и оправданным, поскольку урегулирование указанных отношений будет способствовать эффективной защите прав граждан от незаконного вмешательства в их частную (личную) жизнь, обеспечению разумного баланса публичных и частных интересов, а также соответствовать положениям международных договоров и стандартов. Конкретное изображение гражданина, зафиксированное на материальном носителе, должно охраняться: нормы гражданского законодательства должны не только устанавливать способы такой охраны, но и определять режим использования изображения гражданина другими лицами (аналогично регламенту защиты персональных данных (GDPR), применяемом в Евросоюзе).

Еще одна проблема, ставшая наиболее очевидной в свете событий, произошедших в Беларуси в августе 2020 года, связана с тем, что нормы закона Республики Беларусь от 17.07.2007 № 263-З «Об органах внутренних дел Республики Беларусь» и закона Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации», касающиеся порядка получения, распространения (предоставления) информации о частной жизни и персональных данных сотрудников органов внутренних дел, носят нечеткий и отсылочный характер к иным законодательным актам, которыми такой порядок также не регламентирован, а кроме того не установлен и практический механизм охраны соответствующих гражданских прав.

Общественный совет при Министерстве внутренних дел Республики Беларусь еще в 2018 году в своем обращении в Конституционный Суд указывал на факты самовольного фотографирования и видеосъемки сотрудников органов и подразделений МВД, военнослужащих внутренних войск МВД при выполнении ими служебных задач с последующим распространением и размещением соответствующих материалов в СМИ и сети Интернет. Обстоятельства 2020 года наиболее остро проявили проблему свободного доступа и распространения персональных данных должностных лиц. Тенденциозные подходы к опубликованию изображения влекут максимально негативные последствия, среди – нанесение

непоправимого ущерба имиджу системы правопорядка, правам и законным интересам сотрудников органов и подразделений охраны правопорядка. В связи с этим необходимость обеспечить право граждан на защиту от незаконного вмешательства в их личную жизнь, в том числе сотрудников органов внутренних дел и военнослужащих внутренних войск МВД, находящихся при исполнении служебных обязанностей, устранив неопределенность в правовом регулировании соответствующих отношений, сегодня назрела как никогда.

В связи с указанными обстоятельствами, одним из основных путей решения обозначенных проблем является принятие в целях регламентации отношений, направленных на обеспечение охраны изображения гражданина, Закона Республики Беларусь «О персональных данных», а также включение в ГК соответствующих норм: необходимо установить особенности правового режима использования и охраны изображения гражданина с определением пределов реализации и условий ограничения права на изображение.

Дополнение ГК положениями об охране изображения гражданина должно существенно повысить уровень и эффективность правовой охраны и защиты личных неимущественных прав граждан как нематериальных благ. При подготовке проекта закона Республики Беларусь «Об изменении некоторых кодексов Республики Беларусь» прорабатывался вопрос правового регулирования отношений, связанных с использованием изображения гражданина без его согласия, но было принято решение о нецелесообразности регулирования указанных отношений в ГК в связи с возможностью обеспечения охраны изображения гражданина иными актами законодательства, в том числе Законом «О персональных данных».

В апреле 2021 года во втором чтении Парламентом принят проект закона «О персональных данных». В проекте прописан порядок и цели сбора персональных данных граждан для операторов (сборщиков данных). Кроме того, законодательством предусмотрена как административная, так и уголовная ответственность за утечку данных: все будет зависеть от того, по чьей вине, сколько и в каком объеме незаконно распространено персональных данных, какие последствия наступили в результате этого, однако принятие указанного НПА не отменит необходимость закрепления общих положений о персональных данных как нематериальных благ в ГК.

В текущем периоде принят целый ряд нормативных правовых актов (далее – НПА) в сфере регулирования отношений по защите персональных данных физических лиц от несанкционированного доступа и распространения, а также откорректированы подходы к ответственности за нарушение требований, предъявляемых к использованию персональных данных и национального сегмента сети Интернет.

Среди наиболее важных принятых НПА необходимо отметить внесение изменений в Кодекс об административных правонарушениях Республики Беларусь и подготовку пакета изменений в Уголовный кодекс, принятие указа Президента Республики Беларусь от 16.03.2021 № 107 «О биометрических документах». Кроме того, в развитие указанных документов принята Государственная программа «Цифровое развитие Беларуси» на 2021–2025 годы, в Перечень государственных научно-технических программ на 2021–2025 годы включен пункт 12, предусматривающий программу «Кибербезопасность» (заказчик – ОАЦ, исполнитель – НИИ ТЗИ), а также ряд иных постановлений Правительства: «О порядке использования сведений, содержащихся в материалах оперативно-розыскной деятельности» (от 23.04.2021 № 241), «Об утверждении Соглашения об информационном взаимодействии государств – участников СНГ в области цифрового развития общества» (от 24.02.2021 № 109), «О реализации Указа Президента Республики Беларусь от 18 апреля 2019 г. № 148» – по вопросам функционирования межбанковской системы идентификации физических лиц (от 30 декабря 2020 г. № 773) и проч.

В новых условиях цифровой реальности система права должна гарантировать безопасность реализации прав и свобод человека. Модернизация конституционно-правового статуса личности требует развития правового регулирования с учетом того, что общеправовой принцип свободы личности в настоящее время включает добровольное информированное согласие человека на взаимодействие с информационно-интеллектуальными системами и обязанность государства обеспечить безопасность такого взаимодействия.

ЗАСЕДАНИЕ № 5
КИБЕРБЕЗОПАСНОСТЬ И ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО

УДК 519.876

К ЗАДАЧЕ КОЛИЧЕСТВЕННОГО АНАЛИЗА УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ КВОИ

Н.М. БОБОВИЧ
Учреждение образования «Академия МВД Республики Беларусь, г. Минск, Республика Беларусь

Современные критически важные объекты информатизации (КВОИ) принадлежат к широкому классу систем, обладающих целенаправленным поведением. В процессе функционирования, вследствие воздействия дестабилизирующих факторов и изменения состояния отдельных элементов система, фактически претерпевает случайные изменения своей структуры. Поэтому структурная устойчивость объекта к воздействию дестабилизирующих факторов представляет наибольший интерес при практическом изучении и создании моделей сложных систем в задачах количественного анализа их устойчивости функционирования.

Общей особенностью количественной оценки показателей устойчивости функционировании является статистический характер оцениваемых показателей на всех иерархических уровнях: элемент-подсистема-система в целом. Возможность представления производительности на высших уровнях в виде операторов сопряжения, представляющих собой ее функциональную зависимость от производительностей на более низких уровнях, позволяет свести задачу количественной оценки устойчивости функционирования по показателю «производительность» к задачам расчета статистических характеристик функций случайных аргументов.

Сложность и громоздкость функциональных зависимостей между производительностями элементов и образуемых ими реальных систем существенно затрудняет прямое решение задачи. Для этой цели предлагается использовать метод сопряжения случайных структур (систем) по производительности.

Использование метода анализа случайных структур (систем) по производительности для анализа сложных структур, расчета материального и функционального ущербов, показателя устойчивости функционирования КВОИ основывается на разработке следующего комплекса математических моделей, приведенного на рис.1.

Среди перечисленных моделей особое место в анализе устойчивости функционирования занимает структурно-функциональная модель КВОИ, методика разработки которой и особенности использования приводятся ниже.

Структурно-функциональная модель имеет многоуровневую систему отображения одинаковую по математической структуре на всех уровнях. При переходе от уровня к уровню подсистема низшего уровня принимается элементом на следующем за ним уровне. Многоуровневая система может преобразовываться в одноуровневую путем развертывания подсистем каждого уровня до элементов самого низкого уровня.

Структурно-функциональная модель представляет собой аналитический алгоритм вычисления производительности системы через производительности входящих в него элементов. Разработанная для исследований устойчивости модель имеет графическую форму представления аналитического алгоритма.

Для описания модели и принципов ее построения введем несколько общих определений и терминов:

- система – любая совокупность объектов и элементов;
- подсистема – часть системы;

- элемент – система (подсистема), не подлежащая расчленению (декомпозиции) при ее исследовании;

- структура системы – устойчивая во времени совокупность взаимосвязей между ее элементами (подсистемами);

- оператор сопряжения – аналитический алгоритм, выводящий элемент в систему и его графическое изображение.

В зависимости от характера связей между элементами и подсистемами можно выделить независимые, сложносвязанные, однородные неоднородные и предельные структуры.

Рис. 1. Математические модели метода случайных структур (систем) по производительности

Независимыми будем называть структуры, в которых все параллельные цепи имеют единственный вход и единственный выход. В таких структурах общая производительность связанных элементов определяется независимо от управления в силу отсутствия возможностей перераспределения ресурса между подсистемами. Алгоритм вычисления производительности независимых структур может быть записан непосредственно по графическому изображению путем суммирования производительности параллельных цепей и выбора минимума в параллельных цепях.

Сложносвязанные структуры могут перестраиваться за счет наличия возможностей взаимозаменяемости. Поэтому их производительность будет зависеть от управления ресурсом по заменяемости и может вычисляться только при конкретном фиксированном управлении. Учитывая характер решаемой задачи (оценка устойчивости по максимально сохраняемой производительности), необходимо фиксировать оптимальное управление располагаемым (сохраняемым) ресурсом. При этом условии широкий класс реальных структур может быть преобразован в простейшие последовательно-параллельные (независимые) структуры.

Однородные структуры, в которых любой элемент связан по заменяемости не более чем с одной подсистемой другого наименовании, преобразуются в независимую структуру добавлением одного компенсирующего звена:

$$I = \min_{(i)} \{(\sum_{(j)} K_{ji} I_{ji} + I_i), I^* \} ,$$

где I_{ji} – производительность j-й подсистемы, имеющей заменяемость с i-й подсистемой (может быть нулевой или отличной от нуля);

K_{ji} – коэффициент относительной трудоемкости, показывающий во сколько раз меняется производительность элемента j-й подсистемы при переходе в i-ю подсистему;

I^* – максимально возможная производительность, которая достигается в случае, когда резерв по заменяемости позволяет сбалансировать систему по производительности звеньев.

Неоднородные структуры, которые содержат более сложные и широкие связи преобразуются к последовательно-параллельным аналогам путем последовательного преобразования связей методом преобразования к однородным структурам.

Предельной структурой будем называть систему, содержащую бесконечно большое число невзаимозаменяемых звеньев с бесконечным числом элементов в каждом звене, подвергаемую бесконечно большому числу воздействий.

В силу закона больших чисел число выходящих из строя в такой системе элементов сходится к их математическому ожиданию, а алгоритм расчета производительности позволяет следующее преобразование:

$$M[I] = M\left[\min_{(i)}\{\sum_{(j)} I_{ij}\}\right] = \min_{(i)}\{\sum_{(j} M[I_{ij}]\},$$

не справедливое для ограниченных систем, у которых

$$M[I] < \min_{(i)}\{\sum_{(j)} M[I_{ij}]\}.$$

Полупредельной структурой по числу звеньев будем называть систему с бесконечным числом звеньев и ограниченным числом элементов в каждом звене. Если в такой системе вероятность выхода из строя одновременно всех однотипных элементов не равна нулю, то $M[I] = 0$.

Если существует некоторая предельная производительность, ограничивающая производительность звеньев снизу $(I_{inпред})$, то $M[I] \le I_{inпред}$.

Полупредельной структурой по числу элементов будем называть систему с ограниченным числом звеньев и бесконечным числом элементов в каждом звене. Алгоритм расчета производительности этой структуры совпадает с алгоритмом предельных структур.

Структурно-функциональная модель, построенная по изложенным принципам для некоторой системы, приведена на рисунке 2.

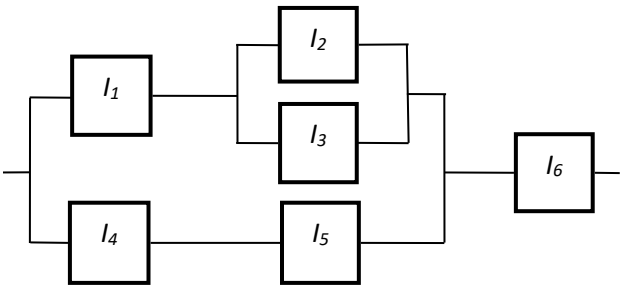


Рис. 2. Структурно-функциональная схема системы

Алгоритм вычисления производительности системы имеет вид

$$I = \min\{[\min(I_1, I_2 + I_3) + \min(I_4, I_5), I_6]\}.$$

Таким образом, метод представления системы в виде совокупности последовательно-параллельных связей между элементами, позволяет установить взаимно-однозначное соответствие между аналитическим выражением оператора сопряжения и его графическим отображением и тем самым дает возможность упростить как задачу записи алгоритмов вычисления производительности, так и расчет ее статистических характеристик. Кроме того, такое представление в ряде случаев позволяет анализировать влияние структуры на устойчивость функционирования системы непосредственно, без ее количественных показателей.

Список литературы

1. Вентцель, Е. С. Теория вероятностей / Е. С. Вентцель – М : Наука, 1969.- 564 с.

2. Александров, Г. В. Методология и инженерные методики расчета живучести сложных систем военного назначения / Г. В. Александров // Научно-методические материалы по оценке эффективности комплексов авиационного вооружения – М. : ВВИА, 1980. – С. 183–197.

3. Бобович, Н. М. Методы оценки ущербов в задачах количественного анализа живучести критически важных объектов информатизации / Н. М. Бобович, В. В. Маликов // Доклады БГУИР. – 2014. – № 4 (82) – С. 59–66.

УДК 004.942

УПРАВЛЯЮЩИЕ ВОЗДЕЙСТВИЯ В СОЦИАЛЬНЫХ СЕТЯХ: АСПЕКТЫ ВЫЯВЛЕНИЯ

Е.П. ОХАПКИНА, А.А. РОГАНОВ
ФГБОУ ВО «Российский государственный гуманитарный университет» (РГГУ), г. Москва, Российская Федерация

Введение. В условиях большого объема информации, представленной в социальных сетях, эффективным подходом к решению задачи выявления деструктивных информационных воздействий является создание системы анализа сетевых сообщений. Стоит отметить, что сетевые сообщения могут включать в себя различные типы контента (текст, аудио, фото, геометки и т. д.). При этом контент может быть представлен как одним из типов, так и сочетанием типов, но в рамках данного исследования будут рассматриваться только сообщения, содержащие текст. Как любая система текстового анализа, система выявления деструктивных информационных воздействий должна включать в себя набор словарей, таких как морфологический словарь, словарь синонимов, словари тональной разметки и ряд других словарей. Поскольку объектом анализа сообщений является словесное выражение, содержащее признаки деструктивного воздействия, то для адекватного заключения о высказывании необходимо в состав словарей также включить словарь паттернов деструктивных высказываний. Поскольку такие словари в открытом доступе отсутствуют и в научных исследованиях не представлены, предлагается подход к построению такого словаря на базе категориального аппарата построения онтологий.

1. **Методология исследования.** Для решения задачи о конструировании семантически зависимых паттернов на русском языке необходимо проделать следующие этапы [1]:

1. Выбор и загрузка модели русского языка, в состав которой входят лемматизатор, токенизатор, POS tagger, модель зависимости слов в предложении;

2. Выбор и подключение к скрипту анализа текста библиотеки, которая сможет использовать загруженную на этапе 1 модель языка. Использовать в анализе означает иметь возможность образовать объект, обладающий всеми атрибутами слов: токен, часть речи (в том числе, для знаков препинания), зависимость слова в предложении, а также атрибуты для программных манипуляций, например, с преобразованием и сравнением слов в предложении и т. п.;

3. Разработка и выявление паттернов, согласно которым из предложения может быть извлечена логически законченная часть высказывания, отражающая главную информационную составляющую.

4. Выбор и подключение специализированных или обобщенных (содержащих в себе как негативные, так и нейтральные или позитивные слова) словарей.

Для анализа использована база данных представляющая собой набор сообщений социальной сети «ВКонтакте» за период 2014 года. База данных сообщений социальной сети «ВКонтакте» насчитывает 262 665 сообщений и 1 127 762 комментария, написанных к ним. Арифметический подсчет покажет, что для предложения со средней длинной 8–12 слов потребуется выполнение от 24 000 до 36 000 операций (проходов с заданными параметрами словаря) на анализ одного сообщения. Таким образом, вычислительный эксперимент по выявлению сообщений и комментариев с признаками агрессии в паттерне составит от 33 до 50 млрд операций (без учета операций парсинга текста, поиска паттернов и записи результата в базу данных). Техническая платформа для выполнения эксперимента: Intel i7 (3.4 GHz, 4 Cores), 6 Gbyte (доступная свободная память с фоновыми рабочими процессами OS Windows).

2. **Конструирование паттернов.** Для конструирования паттернов воспользуемся моделью русского языка SynTagRus.

Предварительно выполним конфигурирование модели русского языка для работы на Python с библиотекой StanfordNLP [1].

```
config = {'proceccors': 'tokenize, mwt, pos, lemma, depparse', 'use_gpu': False,
'lang': 'ru',
'tokenize_model_path': '../ru_syntagrus_models/ru_syntagrus_tokenizer.pt',
'pos_model_path': '../ru_syntagrus_models/ru_syntagrus_tagger.pt',
'pos_pretrain_path': '../ru_syntagrus_models/ru_syntagrus.pretrain.pt',
'lemma_model_path': '../ru_syntagrus_models/ru_syntagrus_lemmatizer.pt',
'depparse_model_path': '../ru_syntagrus_models/ru_syntagrus_parser.pt',
'depparse_pretrain_path': '../ru_syntagrus_models/ru_syntagrus.pretrain.pt'}
```

Здесь в словаре **config** размещаются конфигурационные параметры для подключения модели русского языка (токенизатор, лемматизатор, парсер и др.). После необходимо создать конвейер-обработчик (или pipeline), за счет которого анализируемое предложение, пропущенное через обработчик, получит ряд атрибутов. Ниже показан коду создающий обработчик.

```
snlp = stanfordnlp.Pipeline(**conРисунок)
nlp = StanfordNLPLanguage(snlp)
```

Последняя команда StanfordNLPLanguage позволяет получить класс, с одной стороны, имеющий в распоряжении описанную выше модель русского языка, а, с другой стороны, обладающий методами работы с текстом библиотеки SpaCy [1].

Достоинством применения паттернов является их универсализм по отношению к различным жанрам и тематикам анализируемых текстов. В этом случае актуализации требует только словарь с разметкой негативных слов. Очевидно, что разработка паттернов трудоемкий процесс, но их число счетное и конечное. Чем больше паттернов, тем больше охват извлекаемых фраз и словосочетаний.

Конструкция паттерна может выглядеть, как показано на рисунках 1–3 [1].

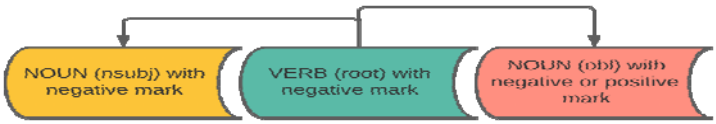


Рис. 1. Шаблон для извлечения сущностей с отрицательным маркером

Рис. 2. Шаблон для извлечения сущностей с отрицательными метками

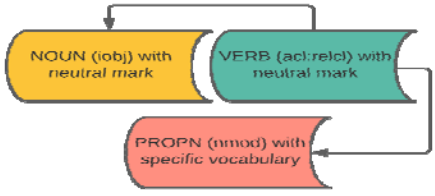


Рис. 3. Шаблон для извлечения сущностей с отрицательными метками

Стоит отметить, что описание свойств (деталей) производимого/описываемого действия/события позволяет более качественно выполнять процедуру выявления деструктивных информационных воздействий в сетевых сообщениях. Например, в сообщении могут быть выделены следующие типы актантов в модели управления [2]:

Быть «агентом» действия;

Быть «объектом» действия;

Быть «адресатом» действия;
Быть «темой» действия;
Быть «инструментом» действия;
Быть «местом» действия;
Быть «начальной точкой» действия;
Быть «конечной точкой» действия;
Быть «целью» действия;
Быть «условием» действия;
Быть «временем» действия;
Быть «способом» действия;
Быть «сроком» действия;
Быть «количеством» действия;
Быть «результатом» действия;
Быть «контрагентом» действия;

Для разработки словаря деструктивных паттернов высказываний использовался онторедактор Protégé 5.5.0. Множество концептов предметной области X включает в себя слова [3], из которых состоят деструктивные паттерны предметной области. Слова включают существительные, глаголы, прилагательные, вспомогательные глаголы, определения, сочетаемые с существительными и другие части речи. В качестве примера на рисунке 4 представлен фрагмент онтологии, включающий в себя три паттерна деструктивных высказываний (Mod_1, Mod_2, Mod_3). В каждый из паттернов включен набор частей речи, и набор лексических правил R их сочетания для образования паттерна, а также задан набор функций интерпретации F.

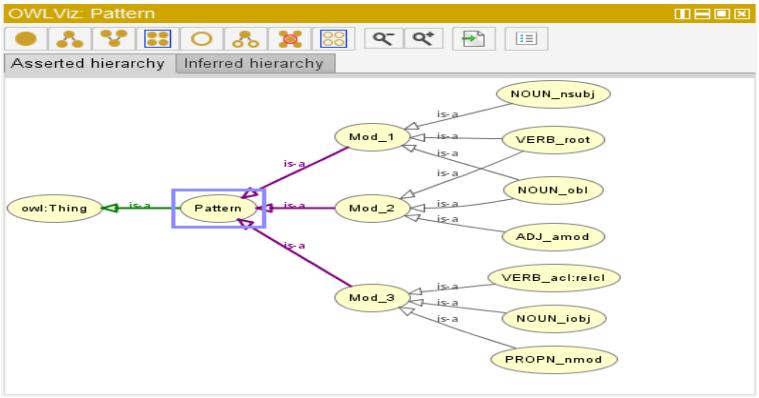


Рис. 4. Фрагмент онтологии паттернов деструктивных высказываний

На рисунке 5 приведен онтограф, представляющий один из частных вариантов сочетания слов, активирующих потенциальное наличие деструктивного паттерна в тексте сообщения. Стоит также отметить, что в качестве части лексического правила для каждого слова указан оттенок или диапазон возможных тональных оттенков слова (см. рисунок 5 красная выплывающая надпись).

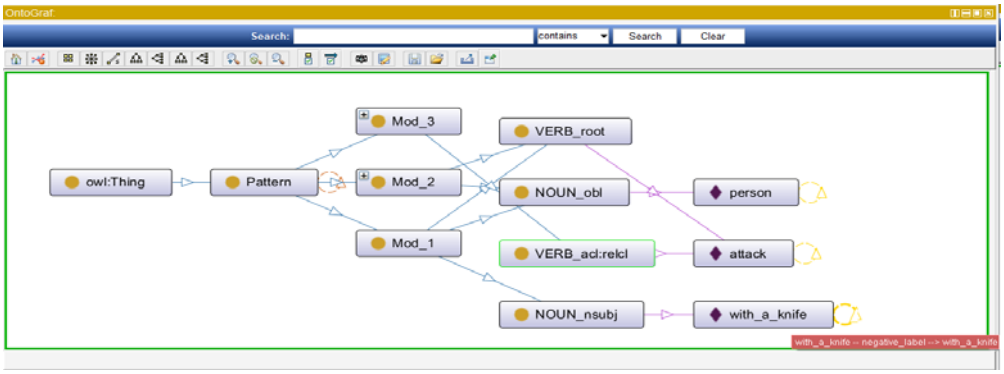


Рис. 5. Пример частной графовой структуры паттерна

Заключение

1. Для построения единого тезауруса важно не только определить лексический состав терминологии, но и используемый набор отношений.

2. Если семантическую структуру определить как сеть семантических отношений, соединяющих единицы знания, то семантические отношения, вводимые в тезаурус, должны моделировать эту структуру.

3. Оценка информационного влияния, как и способы его выявления, зависят, в том числе, от точности настроек алгоритмов обработки текстовой информации: в каком количестве имеются паттерны для обработки текста.

4. В контексте выявления агрессивной, деструктивной информации ключевую роль играет словарь размеченных негативных слов.

5. Именно сочетание «словарь-паттерн» увеличивают возможность точно выявить негативное высказывание и его семантические границы.

6. Конструирование паттернов требует выполнение условия уникальности – паттерн должен быть ориентирован на извлечение фраз и словосочетаний только определенной морфологической конструкции.

Список литературы

1. Okhapkin, V. P. Constructing of Semantically Dependent Patterns Based on SpaCy and StanfordNLP Libraries / V. P. Okhapkin [et al.] // Proceedings International Conference on Futuristic Trends in Networks and Computing Technologies (FTNCT 2020, Taganrog). – Taganrog : Springer, 2021. – P. 500–512.

2. Schütze, H. Introduction to information retrieval / H. Shütze, C. D. Manning, P. Raghavan. – Cambridge : Cambridge University Press, 2008.

3. Цуканова, Н. И. Онтологическая модель представления и организации знаний : учеб. пособие для вузов / Н. И. Цуканова. – М. : Горячая линия – Телеком, 2014.

УДК 004.056

НЕКОТОРЫЕ АСПЕКТЫ ПРОГРАММНО-ЦЕЛЕВОГО ПОДХОДА К РАЗВИТИЮ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Ю.В. БЛИНКОВ
Оперативно-аналитический центр при Президенте Республики Беларусь
г.Минск, Республика Беларусь

Сегодня информатизация стала одним из основных направлений человеческой деятельности и рассматривается как решающий фактор развития общества. Эксперты считают, что к середине XXI века все развитые страны мира осуществят переход к информационному обществу. Однако приход нового общества всегда сопровождается кардинальной ломкой основ старого [1]. Возникают новые технологии управления, которые оказываются настолько эффективными, что старые терпят поражение в конкурентной борьбе. Начинают видоизменятся и перестраиваться структуры управления и взаимодействия в обществе [2].

Это касается всех сторон жизни, в том числе и сферы обеспечения безопасности. Переход к информационному обществу, массовое распространение и доступность информационных технологий приводит к существенному снижению уровня безопасности личности, общества и государства, вызванное невиданной открытостью информационного пространства.

В свое время Республика Беларусь приняла и сегодня реализует идею построения информационного общества. Данное направление является одним из национальных приоритетов. К основным факторам, влияющим на процесс информатизации в нашей стране, следует отнести: выгодное географическое положение республики между информационно-коммуникационными потоками Запада и Востока, а также высокий интеллектуальный уровень общества в целом и персонала, занятого в IT-сфере, – в частности [3].

Одной из важных задач для формирования в республике условий перехода к информационному обществу является развитие нормативной правовой базы. В 1995 г. был принят Закон Республики Беларусь «Об информатизации», в 1999 – Концепция государственной политики в области информатизации.

Государственное регулирование в области информатизации имеют строгую иерархию [4]. Основным нормативным правовым актом в этой области является Закон Республики Беларусь «Об информации, информатизации и защите информации» [5]. В целях совершенствования государственной политике в сфере информатизации принят Указ Президента Республики Беларусь № 531 «О некоторых вопросах информатизации».

Развивается инфраструктура в которой применяются и новейшие технологии. Своевременно решаются вопросы информационной безопасности.

Документом, в котором вопросы информационной безопасности рассматриваются комплексно, стала Концепция национальной безопасности [6]. Согласно концепции, информационная безопасность определяется как «состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере». В дальнейшее развитие правовых основ информационной безопасности Совет Безопасности Республики Беларусь утверждает Концепцию информационной безопасности Республики Беларусь.

Современное общество, развиваясь по пути информатизации, все в большей степени зависит от обеспечения качественной, релевантной, оперативной и достоверной информацией [2]. Эта тенденция затрагивает все сферы деятельности, а обеспечение информационной безопасности стало важным элементом национальной безопасности.

Однако глобальный характер информационного пространства, его открытость и общедоступность представляют собой благоприятную среду для новых угроз и вызовов. Наиболее значимыми в настоящее время считаются угрозы воздействия на информационные

системы и сети государственного и военного управления, системы управления критическими объектами инфраструктуры (энергетика, водоснабжение, воздушное движение и др.), а также массированная психологическая обработка населения в целях дестабилизации общества и государства [2].

Широкое распространение информационных технологий, кроме повышения удобства и эффективного функционирования, и управления, привело к возникновениям и быстрому развитию целого класса новых угроз – «кибернетических».

Вопросы противодействия киберугрозам сейчас прорабатываются в большинстве развитых стран мира. Очевидно, что они должны носить комплексный и системный характер и включать как заблаговременно принимаемые меры, так и меры по активному противодействию в случае выявления фактов кибератак [2].

При этом развитие новых информационных технологий существенно опережает развитие технологий защиты и обеспечения безопасности.

Решение проблем в сфере защиты информации является одним из важных направлений в обеспечении национальной безопасности Республики Беларусь и видится в создании комплексной системы защиты информации. В Республике Беларусь непрерывно и планомерно проводятся мероприятия по созданию безопасного информационного пространства.

В целях решения вышеуказанных проблем выполнялись программы предыдущих периодов: ГНТП «Развитие методов и средств системы комплексной защиты информации» на 2006–2010 годы (ГНТП «Защита информации»), ГНТП «Развитие методов и средств системы комплексной защиты информации» на 2011–2015 годы (ГНТП «Защита информации – 2») и ГНТП «Развитие методов и средств системы комплексной защиты информации и специальных технических средств», 2016–2020 годы (ГНТП «Защита информации – 3»), которые объединили потенциал научных кадров государства, скоординировали усилия научных, научно-исследовательских, научно-производственных и производственных организаций, учреждений и предприятий для решения проблем обеспечения безопасности Республики Беларусь в информационной сфере.

В рамках программ выполнялась разработка научно-технической продукции и нормативно-методической базы для предотвращения следующих угроз: несанкционированный доступ к информации; противоправные сбор и использование информации; внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия; распространение вредоносных программ; утечка информации по техническим каналам; уничтожение и искажение информации; перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации; распространение недостоверной информации.

Для противодействия указанным угрозам в рамках, выполненных ГНТП осуществлен ряд разработок, наиболее значимыми из которых являются:

– аппаратно-программный комплекс криптографической защиты стандартных цифровых потоков Е1;

– информационно-аналитический комплекс, взаимодействующий с системами технических средств по обеспечению оперативно-розыскных мероприятий на сетях электросвязи;

– программное средство обнаружения аномалий операционных систем, причиной которых является присутствие в системе вредоносных программ;

– программный комплекс защиты от вредоносного программного обеспечения, несанкционированного доступа и межсетевого экранирования;

– распределенная система радиомониторинга;

– навигатор систем пространственной локализации источников несанкционированных излучений;

– средства пассивной и активной защиты информации от утечки информации по техническим каналам и ВЧ-навязывания (фильтры-ограничители, генераторы шума);

– программно-аппаратный комплекс для мониторинга, контроля и управления информационными потоками;

– программно-аппаратный комплекс средств гарантированного уничтожения информации;

– система оперативной блокировки вредоносных видов телекоммуникационного трафика;

– аппаратно-программный комплекс распознавания речевой информации.

Указанные разработки внедрены и успешно используются органами государственного управления и государственными организациями Республики Беларусь для обеспечения безопасности в информационной сфере.

Применение разработанных специальных технических средств существенно расширило оперативно-технические возможности специально уполномоченных органов республики, позволило в разы увеличить количество принимаемых и накапливаемых информационных составляющих, повысить эффективность оперативной работы уполномоченных органов Республики Беларусь.

Быстрый темп развития науки и технологий в современном обществе приводит к тому, что технические и программные средства, используемые в информационных системах, постоянно совершенствуются. В связи с этим некоторые разработки, выполненные в рамках программ предыдущих периодов, в настоящее время не могут выполнять в полной мере задачи по своему предназначению. Для устранения указанной проблемы требуется разработка новых средств или переработка (модернизация) имеющихся под новые программно-аппаратные платформы, что практически равнозначно разработке новых средств.

Также в настоящее время по причине расширения использования технических средств и компьютерных технологий в преступных целях и повсеместного внедрения новых методов и способов «информационной войны» необходимо развивать новые направления по борьбе с преступлениями в области информационных технологий в части:

– противодействия компьютерным атакам и распространению вредоносного программного обеспечения;

– выполнения мероприятий по обнаружению и раскрытию каналов обмена информацией между лицами, причастными к преступной деятельности, обнаружению каналов утечки сведений, имеющих ограниченное распространение, выявлению фактов использования электронных средств массовой информации, сетей передачи данных в целях распространения ложной, тенденциозной и другой информации, наносящей ущерб государственным интересам.

Для обеспечения указанных мер требуется разработка средств обнаружения и противодействия компьютерным угрозам, средств анализа и мониторинга активности вредоносного программного обеспечения, средств поиска в программном обеспечении недекларируемых возможностей, совершенствование и разработка специальных технических средств.

В настоящее время сложилась высокая степень зависимости Республики Беларусь от продуктов импортного производства и систем информационных технологий. Республика Беларусь вынуждена идти по пути закупок техники и информационных технологий иностранных фирм-производителей, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации, нарушения функционирования информационных систем и информационно-коммуникационных сетей.

Дальнейшее совершенствование государственной системы защиты информации должно быть направлено на поддержание актуального уровня защиты инфраструктуры страны, уменьшение технологической зависимости в сфере информационных технологий и повышение степени доверия к продукции. Развитие специальных технических средств необходимо проводить с учетом накопленного специфического опыта их применения по пути разработки аналитических систем третьего поколения [7].

Решение данных проблем планируется осуществить путем проведения опытно-конструкторских работ в рамках реализации новой государственной научно-технической программы: «Развитие методов и средств системы комплексной защиты информации и специальных технических средств» («Кибербезопасность»).

Основными целями программы являются:

– обеспечение защиты информации информационной инфраструктуры;

– обеспечение защиты информации информационных систем;

– обеспечение импортозамещения средств защиты информации и специальных технических средств.

Реализация поставленных целей достигается путем выполнения следующих задач:

– проведение опытно-конструкторских работ по созданию средств технической защиты информации, криптографических средств защиты информации, а также специальных технических средств; внедрение полученных результатов; поддержание в актуальном состоянии нормативно-методической базы в сфере технической и криптографической защиты информации в соответствии с полномочиями Оперативно-аналитического центра при Президенте Республики Беларусь, как государственного заказчика.

Указом Президента Республики Беларусь от 7 мая 2020 г. № 156 «О приоритетных направлениях научной, научно-технической и инновационной деятельности в Республике Беларусь на 2021–2025 годы» разработка средств технической и криптографической защиты информации, криптология и кибербезопасность, научное и научно-техническое обеспечение национальной безопасности и обороноспособности государства отнесены к области следующего приоритетного направления научной, научно-технической и инновационной деятельности в Республике Беларусь на 2021–2025 годы: «Обеспечение безопасности человека, общества и государства».

Разработанная государственная научно-техническая программа «Кибербезопасность» является дальнейшим развитием научных разработок по созданию информационных технологий в «защищенном исполнении», средств и систем защиты информации. Она направлена на комплексное решение вопросов обеспечения функционирования национальной государственной системы защиты информации, создание защищенных информационных систем и информационных технологий для органов государственного управления, реального сектора экономики и бизнеса, критически важных объектов информатизации, обеспечение научно-методического руководства и координации работ в области защиты информации в Республике Беларусь.

В программе выделяются следующие направления по развитию методов и средств системы комплексной защиты информации:

– создание технических, программных и аппаратно-программных систем и средств защиты информации, контроля защищенности и оценки эффективности защиты информации;

– создание специальных технических средств;

– развитие защиты информации информационной инфраструктуры и информационных систем;

– поддержание в актуальном состоянии нормативно-методической базы в сфере технической и криптографической защиты информации.

Таким образом, в связи с меняющейся структурой информационных сетей и технических средств их реализации требуется постоянно совершенствовать нормативно-правовую базу, формирующую единую государственную политику в области защиты информации, а также развивать средства защиты информации.

Предполагаемая принципиальная новизна результатов, полученных в ходе реализации программы, будет заключаться в следующем:

– создание системы в целях повышения эффективности анализа вредоносных образцов программного обеспечения, позволяющей эффективно выявлять и классифицировать вредоносное программное обеспечение, базирующейся на определении действий с помощью наборов операционных кодов. Такой подход к выявлению угроз позволяет эффективно обнаруживать и классифицировать обфусцированные вредоносные экземпляры, а также варианты с использованием шифрования строк и ресурсов вредоносного программного обеспечения;

– применение средств искусственного интеллекта (в том числе искусственных нейронный сетей и продукционно-фреймовых систем обработки данных), позволяющих получить гораздо более подробную и релевантную информацию об потенциально

вредоносном образце по сравнению с существующими решениями как в области статического, так и динамического анализа вредоносного программного обеспечения, а также существенно уменьшить временные затраты и нагрузку на аналитика по обработке такой информации;

– разработка программного комплекса в целях защиты от неизвестных вредоносных программ средствами проактивной защиты.

Выполнение в Республике Беларусь ГНТП «Развитие методов и средств системы комплексной защиты информации и специальных технических средств» является актуальной задачей по обеспечению национальной безопасности Республики Беларусь.

Таким образом, обеспечение информационной безопасности осуществляется в соответствии с государственной политикой в данной области, которая включает в себя формирование, совершенствование и реализацию организационных, правовых, научно-технических, правоохранительных, экономических мер обеспечения национальной безопасности в информационной сфере. В свою очередь, именно через развитие этой сферы обеспечивается и ее безопасность.

Государство всесторонне содействует защищенности национальных информационных систем, обеспечению безопасности используемого гражданами и организациями программного обеспечения. В целях улучшения устойчивости государственного сектора к информационным рискам осваиваются передовые технологии, внедряются новые средства и способы обеспечения информационной безопасности. Поощряется развитие технологий безопасности в бизнесе и жизнедеятельности граждан [7].

Список литературы

1. Денисов, А. А. Нетократия и рефлексия: засекречивание в постиндустриальном обществе.
2. Вержбалович, Д. И. Кибервойна. Аспекты безопасности использования информационного пространства.
3. Савицкая, Н. А. Некоторые аспекты построения информационного общества в Республики Беларусь.
4. Указ Президента Республики Беларусь от 6 апреля 1999 г. № 195 «О некоторых вопросах информатизации в Республике Беларусь».
5. Закон Республики Беларусь «Об информации, информатизации и защите информации».
6. Мясникович, М. В. Национальная безопасность Республики Беларусь.
7. Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О концепции информационной безопасности Республики Беларусь».

УДК 004.056

БЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ С ВОЛОКОННО-ОПТИЧЕСКИМИ ТЕХНОЛОГИЯМИ

В.В. ГРИШАЧЕВ
Российский государственный гуманитарный университет,
Институт информационных наук и технологий безопасности,
г. Москва, Российская Федерация

Введение. В современных правовых, нормативных и методических документах делается упор на обеспечение компьютерной безопасности на объектах критической информационной инфраструктуры (КИИ), что объективно отражает современное состояние информационной безопасности (см. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ). Но совершенствование технологической базы информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления приводит к созданию новых ранее неизвестных технических каналы утечки информации. Особую опасность несут технологии реализации информационных процессов на новых физических принципах. В новых технологиях и технике проявляется внутреннее противоречие, связанное с неизученностью всех особенностей функционирования. С одной стороны, внедрение новых технологий создает иллюзию большей защищенности информации, что связывается с новизной используемых принципов, для которых еще не разработаны модели угроз. С другой стороны, существует опасность появления каналов утечки еще не выявленных, функционирующих на физических принципах, не рассматриваемых ранее.

Подобная проблема возникает с применением фотонных технологий в системах сбора, обработки, передачи и хранении информации, в частности, в связи с успешным внедрением волоконно-оптических технологий в системах связи, измерения и безопасности, которые несут значительные преимущества по сравнению с другими технологиями. Решение проблемы возможно при осуществлении физико-технического анализа возможных каналов утечки информации в новых технологиях, построение актуальных моделей угроз, разработке современных технических средств и систем защиты информации, доведение знаний до широкого круга специалистов в области обеспечения безопасности.

1. Информационная безопасность волоконно-оптических технологий. Фотоника одно из основных направлений развития не только в информационной, но и в общей технике. В ней условно можно выделить лазерные, оптоэлектронные, волоконно-оптические и интегрально-оптические технологии. В информатике находит широкое применение волоконно-оптические технологии связи, в настоящее время, кабельные инфраструктуры в основном строятся на волоконно-оптических технологиях. Все новые телекоммуникации проектируются и строятся на оптическом кабеле. Наиболее перспективным абонентским доступом (первая/последняя миля) является оптический доступ в виде пассивных оптических сетей (*Passive Optical Network, PON*), который позволяет оптоволокном связать без промежуточного активного оборудования центральный сетевой терминал с абонентом. В будущем, вся система связи, как локальная, так и дальняя, должна быть полностью оптической (*All-Optical Network, AON*). Доля оптической составляющей в современной связи определяется уровнем развития информационной составляющей на данной территории и непрерывно растет.

Подобная перспектива связана в первую очередь с преимуществами фотонного транспорта над электронным в кабельных сетях. Это меньшие энергетические потери, большая информационная емкость канала связи, долговечность, надежность, инертность к внешним полям и агрессивным средами. Не маловажным преимуществом является отлаженность технологий монтажа и эксплуатации оптических кабельных сетей. Технологичность строительства оптических сетей разного уровня связывается с широким ассортиментом монтажного, испытательного и эксплуатационного оборудования, которое

позволяет проводить строительство подводных, подземных, воздушных телекоммуникаций. Общая протяженность оптических кабельных сетей превышает 4 миллиарда километров, пересекая континенты и океаны.

Кроме информационных коммуникаций, волоконно-оптические технологии находят применение в системах измерений. На оптоволокне можно построить широкий набор датчиков, распределенных измерительных систем практически всех физических величин для механических воздействий, акустических, тепловых, радиационных, электромагнитных полей и т. д. Преимуществом оптоволокна как датчика является высокая чувствительность к внешним полям и воздействиям, распределенность измерений, возможность создания датчика нескольких величин на одном оптоволокне. На основе оптоволокна возможно построение распределенных измерительных сетей для контроля экологического состояния территорий и технологического состояния промышленных объектов. Например, прокладывая оптоволокно внутри дорожного покрытия автострад можно контролировать состояние покрытия. Аналогичные задачи могут решаться в железнодорожном, трубопроводном транспорте, в строительном мониторинге. Одно из важных применений оптоволокна является использование его для решения задач безопасности. Используя преимущества оптического кабеля, его применяют в системах видеонаблюдения, для контроля доступа, охране периметра, в системах пожарной сигнализации и других областях.

Столь широкое распространение волоконно-оптических технологий формирует новые виды угроз безопасности информации на объектах КИИ, которые можно разделить на три направления:

1. Угрозы перехвата трафика в оптических сетях различного назначения;
2. Угрозы несанкционированного сбора информации на объектах критической информационной инфраструктуры через штатные оптические сети;
3. Угрозы применения средств технической разведки (ТР) на основе волоконно-оптических технологий.

Представленная классификация позволяет охватить все аспекты проблемы, каждая из которых имеет самостоятельное значение с некоторой независимой технической реализацией как средств нападения, так и защиты.

2. Угрозы перехвата трафика в оптических сетях. Перехват трафика – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов из информационных сетей.

Оптическая кабельная система объекта КИИ может включать не только телекоммуникационные и локальные сет, но и сети специального назначения такие как телефонной связи, кабельного телевидения, систем видеонаблюдения, различных измерительных систем и другие кабельные системы. Передаваемый по оптическим кабелям трафик носит конфиденциальный характер и имеет важное значение для функционирования объекта не зависимо от вида сети. Трафик может подвергаться различным опасностям, таким как нарушению конфиденциальности, целостности и доступности. Угрозы реализуются различными способами, но одним из основных способов является перехват посредством несанкционированного доступа (НСД) или несанкционированного съема информации (НСИ). При перехвате нарушитель обладает техническими возможностями на уровне современной техники и способен реализовать любой сценарий по получению доступа к конфиденциальной информации, не противоречащий законам физики.

В структуре перехвата важную роль играет способ получения информативных сигналов. Для оптических сетей методы регистрации параметров информативного сигнала можно разделить на контактные и дистанционные. При контактном доступе нарушителю требуется получить физический доступ к оптоволокну в кабеле, что включает необходимость поиска кабеля, разрушения защитных оболочек, выделение требуемого оптоволокна с последующим отводом части оптического информационного сигнала путем (1) разрывы оптоволокна и установки специальной волоконно-оптической вставки или (2) путем воздействия на оптоволокно для вывода части оптического сигнала, например, на изгибе волокна, оптическом туннелировании и др. При дистанционном доступе нарушителю требуется максимально

близкий контакт с оптическим кабелем, только без разрушения или незначительном разрушении его защитных оболочек на основе побочных оптических излучений, паразитных электромагнитных излучений и т. д.

Технические средства защита информации (трафика) могут строиться на особенностях оптического канала связи – его малом поперечном сечении, когда весь информационный сигнал в виде светового потока заключен внутри волокна, кабеля. Первый эшелон защиты связан с техническими средствами контроля доступа к кабелю, к волокну, а также состояния оптического канала связи. Другой способ защиты трафика состоит в зашумлении или искажении сигнала при его передаче в канале связи и очистке от шума или восстановлении его при приеме из канала связи.

В волоконно-оптической линии связи для защиты трафика могут быть применены стандартные методы шифрования, которые применяются для любых других систем связи. В последнее время разрабатываются и предлагаются на рынок системы защиты передаваемой информации от перехвата на основе квантовой криптографии. Есть основания считать такие системы защиты абсолютными по самой природе реализации.

3. Угрозы несанкционированного сбора информации через штатные оптические сети. Несанкционированный сбор (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов из контролируемой зоны КИИ на основе конвергенции функций передачи и измерения в штатных оптических сетях.

На объектах КИИ конфиденциальностью обладает не только внутренний и внешний трафик, но также и информация, циркулирующая внутри объекта в виде речи сотрудников, различных звуков работающего оборудования, физических параметров окружающего пространства и т. д. Штатные волоконно-оптические коммуникации являются распределенной волоконно-оптической измерительной сетью с нештатными измерительными возможностями. Располагаясь внутри объекта КИИ, коммуникации проходят через помещения, в которых может свободно циркулировать конфиденциальная информация. Нарушитель может получить доступ к ней через штатные оптические сети, используя штатные световые потоки сети или внешние зондирующие излучения. В отличие от угрозы трафику, такой канал утечки информации можно считать техническим (ТКУИ), использующим не декларируемые, или не известные, или не контролируемые возможности оптической кабельной инфраструктуры в следствие конвергенции транспортных и измерительных функций сети. Обобщенная структура ТКУИ на основе волоконно-оптических коммуникаций объекта КИИ повторяет схему перехвата трафика, только для формирования сигнала утечки требуется выявить и учесть воздействие на оптоволокно физического поля, связанного с конфиденциальной информации. Воздействие вызывает модуляцию светового потока в оптоволокне, которое переносит информацию за пределы контролируемой зоны, т. е. является информативным сигналом для модулирующего поля. Преобразующие возможности оптоволокна определяют уровень опасности волоконно-оптического ТКУИ. В угрозе безопасности информации большую роль играет топология сети, так как прокладка оптического кабеля вблизи или через охраняемые помещения существенным образом влияет на защищенность от утечек.

Другие особенности связаны с возможностью использования для формирования сигнала утечки в дополнение к штатным излучениям еще и внешних нештатных источников, создающих зондирующие излучения. При этом трудности подключения к оптоволокну сохраняются, оптическая схема может быть усложнена, но повышаются возможности нарушителя путем варьирования параметров источника излучения. Сценарии по реализации ТКУИ через волоконно-оптические коммуникации могут быть различны в зависимости от возможности модуляции света в оптоволокне и целей, преследуемых нарушителем. Здесь играют большую роль специальные сценарии доступа к информации, обсуждение которых наиболее интересно для служб безопасности. Отдельным направлением технической разведки являются волоконно-оптический канал утечки акустической (речевой) информации, который определяется паразитной акустической модуляцией параметров светового потока в оптоволокне.

В этом случае, оптический кабель и его волокна являются нештатным распределенным волоконно-оптическим преобразователем (микрофоном) акустических колебаний воздуха или вибраций конструкций зданий с высокой чувствительностью. Выбор параметров зондирующего сигнала, повышение акустического или виброакустического контакта с оптоволокном, топология и другие обычно не учитываемые характеристики кабельной инфраструктуры позволяет создать высокую угрозу подслушивания конфиденциальных переговоров. Как показывают экспериментальные исследования, наибольшую опасность несут модуляции света на неоднородных участках оптического кабеля, связанные с виброакустическим воздействием, а также возможность применения в качестве средств ТР стандартного волоконно-оптического оборудования, например, волоконно-оптического тестера-телефона с амплитудной модуляцией.

Методы защиты акустической информации от утечки по акустооптическому (волоконному) каналу делятся на пассивные (звукоизоляция оптического кабеля, «правильный» монтаж сети и т. д.) и активные (фильтрация, маскировка, зашумление информационного сигнала и т. д.). Можно выделить еще один способ, заключающийся во включении в каждый оптический трансивер функции непрерывного мониторинга световых потоков на возможность применения технических средств акустической разведки. Уменьшение опасности подслушивания возможно путем разработки новых рекомендаций по монтажу и эксплуатации оптических кабельных систем.

4. Угрозы применения средств технической разведки на основе волоконно-оптических технологий. Преимущества волоконно-оптических технологий может быть использовано для создания волоконно-оптических средств ТР в виде волоконно-оптических датчиков и измерительных систем, адаптированных для выполнения специальных функций. Изначально волоконно-оптические датчики и измерительные системы обладают свойствами, требуемыми для этих целей. Они обладают высокой чувствительностью к широкому кругу физических полей; многофункциональны, т. е. позволяют проводить измерения различных физических величин одним оптоволокном; обладают возможностью как точечными, так и распределенными измерениями; не обнаруживаются стандартными электромагнитными способами, так как не содержат проводящих элементов; пассивны и нечувствительны к внешним электромагнитным полям; пожаро-безопасны; миниатюрны и тд. Все эти преимущества делают их очень эффективным средством ТР. В частности, волоконно-оптические микрофоны уже используются для специальных работ по скрытному подслушиванию переговоров.

В качестве примера одного из направлений применения волоконно-оптических средств технической разведки является возможность повышения эффективности лазерных микрофонов по скрытному дистанционному подслушиванию конфиденциальных переговоров. Одной из трудностей реализации лазерного зондирования вибрирующих поверхностей состоит в высокой ненаправленности отражаемого от неподготовленной поверхности лазерного излучения или наоборот узкой направленности подготовленной поверхности (зеркала). Снятие подобных ограничений можно произвести путем внедрения в стены здания с выделенным помещением сенсорного оптоволокна без защитных оболочек с микролинзами на концах, которые имеют оптический контакт с окружающей средой. Тогда освещение инфракрасным лазерным излучением одного конца на другом конце можно получить модулированное структурным звуком оптическое излучение, которое легко регистрируется как направленное в известном направлении и имеющее известную длину волны лазерное излучение. Противодействие волоконно-оптическим средствам ТР требуют специальных исследований по обнаружению оптического волокна и кабеля, воздействию на его преобразовательную возможность для нейтрализации и др.

Заключение. Представленный анализ информационной безопасности объектов КИИ с волоконно-оптическими технологиями показывает высокий уровень возможных угроз, которые необходимо исследовать, разрабатывать возможные модели угроз, проводить обучение и переподготовку специалистов в данном направлении.

УДК 314/316

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК МЕТОД ИНФОРМАЦИОННОЙ ВОЙНЫ В ФИНАНСОВОЙ СФЕРЕ. АКТУАЛЬНЫЕ ТЕХНИКИ ОБМАНА И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ

А.В. НОВИЧЕНКО
Акционерное общество «Перспективный мониторинг», г. Москва, Российская Федерация

Введение. Стремительное развитие информационно-коммуникационных технологий (далее – ИКТ) стирает существующие национальные границы и транспарентизирует сеть «Интернет». Растущее значение ИБ в экономике, основанной на знаниях, породило обеспокоенность по поводу рисков, связанных с целостностью данных, их конфиденциальностью и доступностью. Кроме того, информационная безопасность также связана с хорошо функционирующей инфраструктурой, которая интегрирована в Интернет.

Современная среда ИКТ характеризуется «повсеместным соединением между гетерогенными сетями и различными системами, и устройствами» [1]. А так, как самым слабым звеном в этой цепочке был и остается человек, то в атаках на финансовые организации в основном применяются методы социальной инженерии (далее – СИ). Атаки с применением методов СИ все чаще применяются не только в преступных целях в рамках общеуголовной преступности, ее следы можно увидеть в атаках, предпринимаемых на финансовые структуры отдельных регионов и целых стран.

Общие сведения о социальной инженерии. Социальная инженерия (далее – СИ) [4] – это термин, используемый для обозначения широкого спектра злонамеренных действий, совершаемых посредством взаимодействия с человеком. Другими словами, это обман, метод манипуляции, использующийся для обмана и получения доступа к информации [9].

Все методы социальной инженерии можно разделить на две больших категории:

1. Методы, основанные на компьютерных технологиях. Злоумышленник должен обмануть жертву, сделав так, чтобы она поверила в то, что на другом конце реальная, верифицированная система. Доверяя системе, жертва выдаст информацию, которую при каких обстоятельствах не разгласила бы.

2. Методы, основанные на человеческом факторе. Злоумышленник использует обман, играет на когнитивных искажениях, чтобы заставить жертву выдать информацию или дать доступ к системе. В данном случае эксплуатируются желание понравиться, склонность быть полезным или невежество жертвы.

Эти «технологии» эксплуатируются как при банальном мошенничестве, так и при целенаправленном деструктивном воздействии на отдельные части финансовой сферы (финансовые организации, банки, государственные финансовые институты).

Для того, чтобы распознавать такие «атаки» и успешно противостоять им, необходимо представлять себе приемы и методы социальной инженерии, используемые злоумышленниками и масштабируемые «заинтересованными» лицами до размеров всей финансовой сферы и ее отдельных объектов, в частности. В целом атаки с применением методов социальной инженерии являются, по сравнению с техническими, наиболее успешными. Это происходит, в том числе и потому, что специалисты по безопасности, как правило, упускают из вида риск применения методов социальной инженерии. Так же злоумышленник играет на привычках и природе человека, люди склонны действовать «по умолчанию», способность к критическому мышлению у многих находится в зачаточном состоянии, а то и вовсе «отключена».

Этапы социальной инженерии. Социальная инженерия как использование ограниченности человеческого мышления не претерпевала изменений на протяжении веков. Изменяются лишь отдельные нюансы, основная идея остается неизменной. Этапы тоже неизмен-

ны и их можно разделить на предварительный сбор информации, развитие доверительных отношений и эксплуатацию.

Сбор информации. В настоящее время, когда ежесекундно загружается полторы тысячи фотографий в Instaram, публикуется 8 000 твитов, сбор информации не кажется сложным делом. Претекстинг, т. е. первоначальный сбор информации об объекте, к которому будут применены методы СИ в наше время очень прост. Социальные сети, мессенджеры, другие ресурсы, предоставляют злоумышленнику возможность составления образа будущей жертвы в любой плоскости – социальной, профессиональной или технической. Любая информация о жертве может стать ключом к успешной атаке, даже если она выглядит недостаточно важной. Это может быть простая личная информация, фотографии, данные о местоположении, дружеские связи, деловая информация и многое другое. Злоумышленник может собрать всю доступную информацию воедино и создать образ, который можно использовать для совершения атаки. Это может помочь убедить жертву в том, что она общается с каким-то конкретным человеком или в том, что ей может стать известна какая-то инсайдерская информация, могущая принести прибыль.

Развитие доверительных отношений. На этом этапе злоумышленник развивает отношения с жертвой, выставляя себя опытным и авторитетным человеком. В основном это делается с помощью, ранее собранной или инсайдерской информации. В некоторых случаях активно используется инерция человеческого сознания – если человек говорит, что является кем-то, то это, как правило, принимается на веру. Также может использоваться лень, страх неприятностей, склонность доверять, если что-то говорится уверенным тоном или если собеседник апеллирует к признанным авторитетам.

Эксплуатация отношений. Эксплуатируя уже полученное преимущество, злоумышленник сосредотачивается на поддержание у жертвы ощущений, вызванных нарисованным образом. Путем манипуляций, злоумышленник старается привести жертву в определенное эмоциональное состояние. Путем использования так называемых «когнитивных искажений» атакующий не только изучает эмоциональное состояние жертвы, но и использует его в своих интересах. Список когнитивных искажений [5], обширен и включает в себя огромное количество устойчивых стереотипов и установок, имеющихся в мышлении практически каждого человека. Социальная инженерия позволяет атакующему использовать противоречия в мышлении, устоявшиеся штампы. В некоторых случаях злоумышленник оставляет у жертвы ощущение того, что он сделал что-то хорошее. В таком случае у атакующего имеется возможность несколько раз использовать помощь жертвы в получении информации.

Методы социальной инженерии

1. Подначивание. Жертва разглашает информацию, которую она бы не разгласила ни при каких

2. Желание обладать чем-то редким. Злоумышленник играет на желании жертвы получить то, что отсутствует у остальных, будь то статус или какая-либо информация.

3. Обратная социальная инженерия. Злоумышленник создает у жертвы впечатление, что он наделен административными или техническими полномочиями, чтобы жертва просила у него помощи.

4. Фишинг. Самый популярный метод получения доступа к информации, заключающийся в использовании поддельных идентификаторах вызывающего абонента, чтобы создать впечатление, что звонки поступают из облеченной доверием организации. Фишинг может быть проведен с использованием электронной почты, SMS-сообщений, голосовой почты или звонками на мобильный номер жертвы.

5. Целевой фишинг. Этот метод заключается в использовании ранее собранной информации и отправлении кастомизированного сообщения конкретному лицу. Уровень успешности у такого метода намного больше, чем при массовой рассылке большого количества не персонализированных сообщений.

6. Атака «на водопое». У жертвы создается впечатление, что она использует те ресурсы, которым доверяет. Огромное количество фальшивых ресурсов ждут, когда жертва, введенная в заблуждение, введет свои данные, после чего злоумышленник может использовать

из в противоправных целях. Или же злоумышленник может внедрить вредоносное программное обеспечение, которое жертва распознает как настоящее и предоставляет доступ к защищенной системе или к конфиденциальным данным.

7. «Заторапливание». Метод, заключающийся в создании состояния спешки и нагнетания паники, под воздействием которых жертва принимает неверные решения, т. е. поступает так, как нужно злоумышленнику.

Примеры атак с применением социальной инженерии на объекты финансовой сферы. Бытовой уровень:

1. Отдельные эпизоды мошенничеств с гражданами, которые, однако, складываются в целые мошеннические компании.

2. Хакерские атаки на банковские приложения.

Атаки на отдельные финансовые организации:

1. Атаки путем распространения ложной информации о неустойчивости финансовой организации.

2. Атаки путем распространения заведомо ложной информации в средствах массовой информации о ключевых персонах финансовой организации.

3. Хакерские атаки на информационную инфраструктуру банка

Атаки на финансовую сферу. Атаки на финансовую сферу государства – это «игра вдолгую». Никакими скорыми мероприятиями нельзя достигнуть больших результатов, поэтому «злоумышленник» подтачивает финансовое благополучие государства малыми, незаметными действиями. Утрата доверия к финансовой системе государства или к банковской системе, повышение уровня инфляции, падение покупательской способности отдельных слоев населения, все это ясно видимые следы операций, результатом которой может стать полная утрата доверия населения к финансовой системе государства, и, как следствие, повышение протестной активности населения.

Методы противодействия. На уровне отдельных мошенничеств:

1. Наглядная агитация

2. Инструктажи персонала (возможно, стимулирование сотрудников финансовых организаций при выявлении преступлений)

3. Социальные видеоролики в средствах массовой информации, особенно – на телевидении и радио.

4. Повышения финансовой грамотности различных слоев населения.

5. Активная работа с органами внутренних дел, направленная на повышение эффективности работы с населением, а также на облегчение работы оперативных подразделений по уже совершенным преступлениям.

На уровне атак на финансовые организации:

1. Мониторинг публикаций в средствах массовой информации федерального, регионального и местного масштаба.

2. Управление репутацией путем работы с отзывами в средствах массовой информации, социальных сетях.

3. Проведение всестороннего анализа утечек и атак с применением информационно-аналитического программного обеспечения.

4. Повышение грамотности персонала финансовых организаций, информирование о методах социальной инженерии, используемых при совершении противоправных деяний.

5. Проведение на регулярной основе тренировок с техническим персоналом, направленных на повышение знаний по противодействию как техническим атакам, так и атакам с использований методов социальной инженерии.

На уровне атак на финансовую сферу:

1. Активное участие государственного регулятора на предмет внесения изменения изменений в законодательную базу.

Этим уже занимается Центральный банк Российской Федерации, но, как мы видим, этих усилий недостаточно:

ЦБ предложил внести телефонное мошенничество в Уголовный кодекс [6]

Банк России предлагает подвести телефонных мошенников под статью 159.6 Уголовного кодекса «Мошенничество в сфере компьютерной информации». Максимальное наказание по этой статье – 10 лет лишения свободы.

Банк России неоднократно выступал за ужесточение ответственности в этой сфере. Еще в 2019 году рассматривалось введение отдельного состава преступления для сотрудников и организаторов мошеннических кол-центров.

2. Повышение компетенций подразделений финансовых организаций, ответственных за защиту внутренней структуры, а также проведение регулярного аудита (пентеста)не только внутренней структуры, но и финансовых приложений (online-банкинг, инвестиционных приложений).

3. Проектирование и реализация единой финансовой информационной структуры, подобной ФинЦЕРТ, охватывающей финансовые структуры союзных государств. В случае получения информации о совершении атаки на ФО одного из участников структуры, информация о ней и мерах противодействия должна быть доступна всем.

Заключение. Приведенный выше список мер противодействия далеко не исчерпывающий. Его реализация, а также разработка комплекса мер по противодействию новым угрозам являются крайне необходимыми для гармоничного развития и обеспечения стабильности финансового рынка, платежных систем, укрепления банковской системы и развития экономики не только Российской Федерации, но и других стран постсоветского пространства.

Список литературы

1. Бандурко, С. А. Информационный риск в банковской деятельности : автореф. … канд. экон. наук. Санкт-Петербургский гос. экон. ун-т. СПб., 2020 г. [Электронный ресурс] / С. А. Бандурко. – Режим доступа : https://www.dissercat. com/content/informatsionnyi-risk-v-bankovskoi-deyatelnosti. – Дата доступа : 30.04.2021.

2. Кабанов, Ю. А. Информационное пространство как новое (гео)политическое пространство: роль и место государств [Электронный ресурс] / Ю. А. Кабанов // Сравнительная политика. – 2014. – № 4 (17). – Режим доступа : https://cyberleninka.ru/article/n/informatsionnoe-prostranstvo-kak-novoe-geo-politicheskoe-prostranstvo-rol-i-mesto-gosudarstv. – Дата доступа : 19.04.2021.

3. Основные типы компьютерных атак в кредитно-финансовой сфере в 2019–2020 годах [Электронный ресурс] // Центральный банк Российской Федерации. Москва, 2021 г. – Режим доступа : https://www.cbr.ru/Collection/Collection/File/32122/Attack_2019–2020.pdf (дата обращения 01.05.2021).

4. Социальная инженерия [Электронный ресурс]. – Режим доступа : https://www.imperva.com/learn/application-security/social-engineering-attack/. – Дата доступа : 19.04.2021.

5. Список когнитивных искажений, улучшенная версия [Электронный ресурс]. – Режим доступа : http://metaver.pbworks.com/w/page/Список%20когнитивных%20искажений%2C%20улучшенная%20версия. – Дата доступа : 20.04.2021.

6. ЦБ предложил внести телефонное мошенничество в Уголовный кодекс [Электронный ресурс]. – Режим доступа : https://rg.ru/2021/03/25/cb-predlozhil-vnesti-telefonnoe-moshennichestvo-v-ugolovnyj-kodeks.html

7. Vishik, C. Key Concepts in Cybersecurity: Towards a Common Policy and Technology Context [Electronic resource] / C. Vishik, M. Matsubara, A. Plonk //International Cyber Norms: Policy, Legal, and Industry Perspective. – 2016.

8. ЦБ предложил внести телефонное мошенничество в Уголовный кодекс [Электронный ресурс]. – Режим доступа : https://rg.ru/2021/03/25/cb-predlozhil-vnesti-telefonnoe-moshennichestvo-v-ugolovnyj-kodeks.html. – Дата доступа : 03.05.2021.

9. Social Engineering Threat and Defense : A Literature Survey [Electronic resource] // Journal of Information Security 09(04):257-264. – Режим доступа : https://www.scirp.org/journal/paperinformation.aspx?paperid=87360. – Дата доступа : 28.04.2021.

10. The 7 Deadly Sins of OSINT [Electronic resource]. – Режим доступа : https://www.secjuice.com/the-7-deadly-sins-of-osint. – Дата доступа : 02.05.2021.

УДК 004.054.5

ПОСТРОЕНИЕ НАЦИОНАЛЬНОЙ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ

А.В. ДЕНИСЕВИЧ
Оперативно-аналитический центр при Президенте Республики Беларусь, г. Минск, Республика Беларусь

Изучение специальной литературы показало, что в современных условиях каждая организация заинтересована в эффективном управлении своей информационно-аналитической деятельностью. В частности, конкурентоспособность государства в значительной степени зависит от уровня информационной безопасности. Именно он и определяет защищенность национальных и частных интересов от неблагоприятного воздействия факторов внешней и внутренней среды.

В настоящее время определяющим фактором для информационной безопасности Республики Беларусь является активное внедрение информационно-телекоммуникационных технологий на основе технологии блокчейн и больших данных во все сферы жизнедеятельности общества, в первую очередь в республиканские органы государственного управления и кредитно-финансовую сферу. Перечисленные технологии представляют собой совокупность программных, технических и организационно-экономических средств, объединенных структурно и функционально для решения задач передачи и обработки информации. Однако до сих пор не решены такие комплексные вопросы, как обеспечение информационной безопасности Республики Беларусь, создание системы информационной безопасности и ее финансирования. На законодательном уровне не установлено за счет каких финансовых средств будет осуществляться построение системы информационной безопасности, как критически важных инфраструктур, так и страны в целом, отсутствует разработанный план обеспечения и восстановления информационной безопасности государства.

Другими словами, на практике защита информации представляет собой комплекс регулярно используемых средств и методов, принимаемых мер и осуществляемых мероприятий с целью систематического обеспечения требуемой надежности информации, генерируемой, хранящейся и обрабатываемой в информационной системе, а также передаваемой по каналам связи. Для получения наилучших результатов защита информации должна носить комплексный характер, то есть все разрозненные виды защиты информации должны быть объединены в одно целое и функционировать в составе единой системы защиты информации, представляющей собой слаженный механизм взаимодействующих элементов, предназначенных для выполнения задач по обеспечению безопасности информации.

Более того, комплексная система защиты информации должна обеспечивать, с одной стороны, функционирование надежных механизмов защиты, а с другой, управление механизмами защиты информации. В связи с этим, необходимо отметить, что актуальным сегодня является создание теории информационной безопасности, так как развитию теоретической базы данной сферы в Республике Беларусь уделяется недостаточно внимания, в том числе и вопросу подготовки профессиональных кадров в данной сфере.

Заметным недостатком толкования концепции правовых мер является исторически сложившееся доминированием технических мер по защите информации. Правовые меры должны также включать разработку стандартов, устанавливающих ответственность за компьютерные правонарушения, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, судопроизводство и принятие соответствующих международных актов. Законодательное регулирование отношений между субъектами гражданских правоотношений, авторских прав, а также установление защитных норм административного и уголовного законодательства в случае нарушения установленных законом правил обращения или защиты информации, таким образом, представляет собой совокупность правовых мер используемых для защиты информации. Наличие стабильной и хорошо регламентированной правовой базы гарантирует успех в достижении целей максимальной защиты законных интересов владельцев информационных прав (как реальных, так и нематериальных).

Таким образом, проблема обеспечения информационной безопасности сегодня как никогда актуальна и требует комплексного решения. При этом значительно расширился круг задач, выполнение которых необходимо в ходе обеспечения безопасности информации. Недостаточно просто обеспечить доступ к информации только санкционированных пользователей и запретить доступ пользователей, не имеющих на то соответствующего права. Необходимо, в случае обнаружения факта несанкционированного доступа, получить информацию о самом нарушителе, преследуемых им целях, его местонахождении, дезинформировать и дезориентировать нарушителя, перенаправив его информационный поток на специально созданный «ложный объект атаки», а также по характерным действиям нарушителя своевременно обнаруживать и предотвращать попытки несанкционированного доступа в дальнейшем.

Закономерным итогом проведения планомерной государственной политики в сфере защиты информации явилось принятие Концепции информационной безопасности, представляющую собой систему официальных взглядов на сущность и содержание обеспечения национальной безопасности в информационной сфере, определяет стратегические задачи и приоритеты в области обеспечения информационной безопасности. Документ обеспечивает комплексный подход к проблеме информационной безопасности, создает методологическую основу для совершенствования деятельности по ее укреплению, служит основанием для формирования государственной политики, выработки мер по совершенствованию системы обеспечения информационной безопасности, конструктивного взаимодействия, консолидации усилий и повышения эффективности защиты национальных интересов в информационной сфере.

Проведенный анализ развития понятия персональных данных показал, что развитие отечественного законодательства идет по пути постепенного расширения круга сведений, признаваемых персональными данными, а также восприятия подходов к определению персональных данных, закрепленных в международных нормативных правовых актах. Национальное законодательство о персональных данных отличается крайней разрозненностью и фрагментарностью, наличием ряда невыполнимых норм (например, о необходимости получения согласия на действия с персональными данными только в письменной форме), отсутствием действенных механизмов привлечения к ответственности за допускаемые нарушения. В связи с этим требуется комплексное реформирование данного института законодательства в целях обеспечения действенного механизма защиты прав субъектов персональных данных. Важнейшим элементом такого механизма должен стать общий закон о защите персональных данных.

При выработке новых рамок правового регулирования работы с персональными данными следует учесть сложности, с которыми сталкиваются другие страны в применении законодательства о персональных данных (расплывчатость границ понятия персональных данных, тенденция постоянного расширения указанного понятия с учетом развития информационных технологий, несовместимость природы отдельных технологий, в частности Больших данных, интернета вещей, с базовыми принципами работы с персональными данными).

В любом случае выбираемая модель регулирования персональных данных должна основываться на идее баланса между интересами оператора и субъекта персональных данных. С одной стороны, установленные ограничения на обработку персональных данных и предоставленные субъекту персональных данных права должны обеспечить контроль за использованием персональных данных, а с другой – исключение излишних обременений должно оставлять возможность для развития информационного общества с использованием новых технологий.

Для устранения серой зоны нормативного правового регулирования с целью обеспечения соответствующего международным нормам и стандартам уровня охраны и защиты персональных данных граждан в Республике Беларусь, для создания эффективной системы охраны и защиты персональной информации, а также исключения информационной изоляции на международном уровне (невозможностью реализации совместных межгосударственных проектов, связанных с наличием (передачей) информации о персональных данных) Республике Беларусь необходимо присоединиться к Конвенции Совета Европы 108 от 28 января 1981 года «О защите частных лиц в отношении автоматизированной обработки данных личного характера».

В рамках рассмотрения особенностей сферы защиты информации можно сделать вывод о многогранности затрагиваемых вопросов регулирования технической и криптографической защиты информации, которая затрагивает и оказывает воздействие на большое количество сфер деятельности таких как: лицензирование, сертификация, обеспечение государственных информационных систем обрабатывающих служебную информацию ограниченного распространения, обеспечения безопасности критически важных объектов информатизации. В связи с чем можно сделать вывод о разнообразности решаемых вопросов законодательством в сфере защиты информации.

Законодательство, затрагивающее вопросы защиты информации, претерпело изменение в конце 2019 года. Однако заметные отличия фактически отсутствуют, за исключением вопросов, затрагивающих безопасность КВОИ, где заметны существенные изменения регулирования данного вопроса. Вышеназванные изменения объясняются необходимостью уточнить критерии, на основании которых объекты информатизации относятся к критически важным. Государственные органы по ряду причин субъективного и объективного характера не относили отдельные объекты информатизации к критически важным. Уточненные критерии и показатели уровня ущерба в различных сферах должны способствовать тому, чтобы эти объекты вошли в реестр критически важных.

Кроме того, в соответствии с требованиями времени назрела насущная необходимость обновить механизмы повышения надежности критической информационной инфраструктуры. Это тем более важно, если учитывать новые риски и угрозы информационной безопасности.

Таким образом к сложностям сферы защиты информации можно отнести многогранность затрагиваемых вопросов регулирования технической и криптографической защиты информации, лицензирования, сертификации и обеспечения безопасности критически важных объектов информатизации. Завершился длительный процесс совершенствования законодательства в сфере обеспечения безопасности КВОИ, который проводился для создания наиболее эффективной правовой базы, соответствующей современным вызовам и угрозам национальной безопа сности Республики Беларусь.

Результатом проведенной работы стала наглядность проблемных вопросов регулирования сферы защиты информации, таких как сертификация средств защиты, лицензирование деятельности по технической и криптографической защите информации, обеспечение безопасности критически важных объектов информатизации. Для решения данных вопросов необходимо проводить совершенствование законодательства в данной сфере на регулярной основе один раз в три-четыре года, а не раз в семь лет. Так как развитие информационной сферы происходит стремительно, а, для того чтобы соответствовать новым вызовам и угрозам в информационной сфере необходимо иметь гибкое, современное и соответствующее духу времени законодательство в сфере защиты информации. Для этого необходимо возможность применения зарубежных стандартов в сфере информационной безопасности: NIST и ISO/IEC, которые уже опередили развитие национального законодательства на десятилетия вперед, в таких вопросах как безопасность интернета вещей, умный город и т. д. В целях своевременного устранения проблемных областей законодательства необходимо иметь актуальное и современное информационно-аналитическое обеспечение подразделений, осуществляющих регулирования сферы защиты информации.

Список литературы

1. Указ Президента Республики Беларусь от 9 ноября 2010 г. №575 «Об утверждении Концепции национальной безопасности Республики Беларусь»

2. Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. №1 «О Концепции информационной безопасности Республики Беларусь»

3. Указ Президента Республики Беларусь № 196 «О некоторых мерах по совершенствованию защиты информации»

4. Конвенция Совета Европы 108 от 28 января 1981 года «О защите частных лиц в отношении автоматизированной обработки данных личного характера»

5. Закон Республики Беларусь от 19 июля 2005 г. № 45-З «Об электросвязи»

6. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449»

7. Абламейко, М. С. Правовое обеспечение информационной безопасности при формировании информационного общества в Республике Беларусь / М. С. Абламейко, Д. А. Марушко // Вес. Нац. акад. навук Беларусі. Сер. гум. навук. – 2011. – №4. – С. 39–45.

УДК 519.81

ВЛИЯНИЕ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ И КОММУНИКАЦИИ НА ПОВЕДЕНИЕ БОЛЬШИХ СОЦИАЛЬНЫХ ГРУПП

А.Н. НАСЕВИЧ, Е.А. РАФАЛЬСКАЯ
Государственное учреждение «Научно-исследовательский институт Вооруженных Сил Республики Беларусь», г. Минск, Республика Беларусь

Основные теоретико-методологические вопросы провоцирования негативных эмоциональных состояний, а также прикладные аспекты деструктивного поведения различных категорий граждан Республики Беларусь, в том числе лиц, принимающих решения, формируемых под воздействием средств массовой информации и коммуникации (СМК), в настоящее время довольно хорошо изучены. Однако массовидные явления, связанные с изучением свойств больших социальных групп (БСГ), имеют свои характерные особенности, что не позволяет использовать существующие модели и методики в отношении прогнозирования их поведения.

В качестве примера следует привести слова С.П. Расторгуева «Информационное противоборство, являясь составной частью общего противоборства, имеет свои специфические события, знания о которых позволяют судить о ведении информационного противоборства. В общем случае проблема выявления факта начала информационной операции относится к алгоритмически неразрешимым проблемам, но на определенном этапе развития информационной операции появляются признаки, позволяющие получать вероятностные оценки факта ее проведения…». Исходя из изложенного следует, что выявление прикладных аспектов провоцирования негативных эмоциональных состояний (ЭС) в БСГ и исследование их поведенческих реакций является важной и актуальной задачей.

Циркулирующие в информационном потоке сообщения актуализируют социальные и социокультурные ценности и символы (образы) в БСГ, редуцируя определенные паттерны поведения. Соответственно, оценка результатов деятельности органов военного управления по нейтрализации информационно-психологических воздействий (ИпВ) на информационно-психологические объекты, в качестве которых рассматриваются выделенные категории граждан республики (БСГ), зависит от канала(ов) доведения информации. В этой связи следует отметить, что современное общество реальным воспринимает только то, что продемонстрировано по телевидению, озвучено на радио, прочитано в прессе и Интернете, а также услышано от знакомых людей.

Следует отметить, что эмоциональные состояния больших социальных групп лежат в основе их поведения и зависят от целого ряда факторов, оказывающих влияние на все слои общества. При этом выделяют *внутренние и внешние факторы*.

К **внутренним факторам** относятся:

а) социально-экономическое состояние общества: уровень доходов населения, удовлетворенность материальным положением, безработица, социальные гарантии, миграция, инфляция, доходы населения с величиной минимального потребительского бюджета, соотношение *«богатых» и «бедных»,* уровень образования, здравоохранения и другие показатели, характеризующие уровень жизни населения;

б) *политическое состояние общества:* соблюдение прав и свобод граждан; доверие к органам государственного управления, социальным институтам, политическим партиям, общественным организациям; коррупция, бюрократия, государственная идеология;

в) состояние (уровень) безопасности общества, представляющее угрозу жизни и здоровью населения: военная угроза, уровень преступности, санитарно-эпидемиологическое состояние, климатические катаклизмы, катастрофы, аварии техногенного характера;

г) существенные изменения, повлекшие снижение социального статуса или благополучия больших социальных групп: повышение (понижение) пенсионного возраста, зарплат и налоговой нагрузки, ущемление прав и свобод отдельных БСГ или всего общества;

д) значимые общественно-политические события: референдумы, выборы руководителей государств или представителей органов власти, демонстрации, публичные выступления, марши, забастовки, непропорциональное применение силы правоохранительными органами.

Основными **внешними факторами** являются:

а) информационно-психологические воздействия на социально значимые ценности населения: фальсификация исторических событий, героизация (обеление) изменников Родины наряду очернением подвигов и заслуг выдающихся государственных деятелей, насаждение западной массовой культуры и ценностей, формирование общества *«потребителей»,* размывание традиционных, базовых ценностей в отношении брака и семьи, религии, подмена образов, стереотипов, понятий, формирующих мировоззренческие основы общества. Кроме того, к ним относятся: *воздействие* на политических деятелей, представителей элиты государства (преследование, санкции), формирование образа *«страны-изгоя», «оси зла»*;

б) социально-экономические воздействия: экономические санкции, эмбарго, ограничение на перемещение в страны Евросоюза и т. д.

Не дифференцируя отдельные состояния больших социальных групп общей характеристикой эмоциональное состояние, в значительной степени определяющее их поведение, можно выделить *«общественное настроение».* Подобное эмоциональное настроение определяется не каким-либо конкретным событием или явлением, а формируется под влиянием выделенных внутренних и внешних факторов, характеризуясь эмоциональным фоном и динамикой. Соответственно, высокий уровень негативности эмоционального фона провоцирует усиление протестного потенциала общества.

Показателем общественного настроения является *коэффициент негативности общественного настроения* [1], который характеризует интенсивность выраженности эмоциональных переживаний населения и может находиться в диапазоне от нуля (полное спокойствие, безразличие, т. е. отсутствие эмоционального реагирования) до максимальной величины эмоционального реагирования. Он выражается в относительных единицах. Чем выше значение этого показателя, тем интенсивнее негативный эмоциональный фон. Существует некоторый критический момент, когда уровень эмоционального фона достигает порогового уровня, за которым следуют протестные действия. Следует отметить наличие корреляционной зависимости между уровнем негативности общественного настроения и уровнем протестного потенциала общества.

В подтверждение изложенному, на рисунках 1 и 2 представлены графики динамики изменения негативности общественного настроения и протестного настроения соответственно в Российской Федерации с 1992 по 2012 гг. [1].

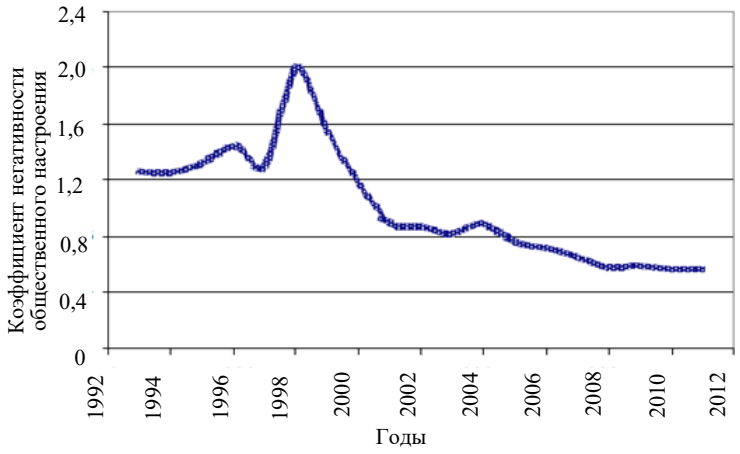


Рис. 1. Динамика негативности общественного настроения в РФ

Согласно рисунку 1 коэффициент негативности общественного настроения имеет максимальное значение в 1998 г. и, как следствие, в 1999 г. наблюдается максимальный уровень протестного потенциала общества (рис. 2). В 2004 г. аналогичное усиление негативности общественного настроения послужило толчком к увеличению протестного потенциала в 2005 г. [1].

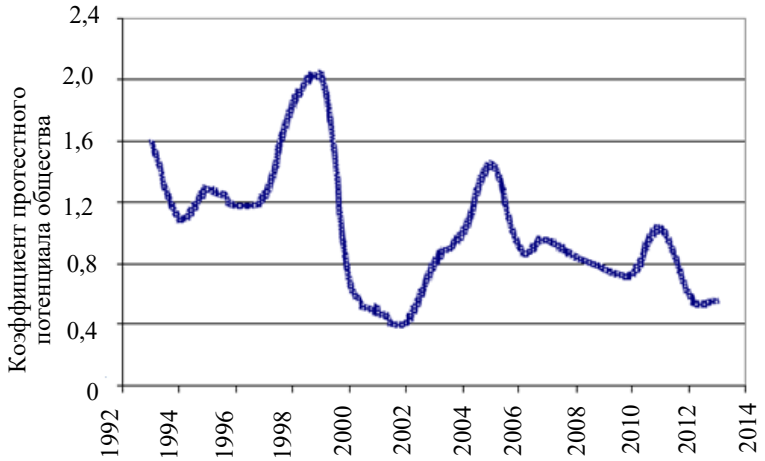


Рис. 2. Динамика протестного потенциала общества в РФ

Динамика коэффициента протестного потенциала общества соответствует динамике показателей общественного и личного протестного потенциала. На графике прослеживается несколько периодов. Заметные усиления протестной активности наблюдались с 1998 по 1999 гг., в 2005 и 2011 гг., а спад отмечался в 2000 г. В целом протесты выше среднего уровня были зафиксированы в период с 1993 по 1999 гг., с 2004 по 2005 гг. и в 2011 г.

Таким образом, эмоциональное состояние общества формируется под непрерывным воздействием внутренних и внешних факторов. Знание особенностей данного влияния, следствием которого является практически прямая зависимость протестного потенциала в обществе от общественного настроения, позволяет прогнозировать и предупреждать негативное развитие социально-политической и информационной обстановки в обществе, своевременно планировать и проводить комплекс мероприятий по снижению уровня эмоциональных состояний негативной направленности БСГ.

Поскольку Республика Беларусь, как и другие постсоветские страны, интегрирована в глобальное информационное пространство, где доминирует контент Запада в культурологическом и технологическом плане, то и в нашей стране происходят события, связанные с негативными информационно-психологическими воздействиями или на все общество или на отдельные социальные группы. Можно констатировать тот факт, что с использованием соответствующие технологии, направленных на изменение базовых ценностей общества, сформировано протестное движение. Немаловажное значение при этом сыграли средства массовой информации и коммуникации.

Следует отметить, что данное протестное движение сформировано не в одночасье. Да, внутренние факторы, отмеченные выше, привели к росту негативизации в обществе, росту недоверия к институтам власти и органам государственного управления. В качестве основных факторов следует отметить снижение доверия к Центральной избирательной комиссии, Правительству и непосредственно Президенту Республики Беларусь на фоне пандемии, снижения уровня финансовой обеспеченности большинства граждан республики, заметного расслоения общества, создание «привилегированного» класса, уровень жизни которых заметно превышает уровень большинства граждан Беларуси.

Однако, на наш взгляд, данные факторы не привели бы к массовым выступлениям, если бы отсутствовало целенаправленное информационно-психологическое воздействие на большие социальные группы, практически все слои населения по всей республике. В связи с вышеизложенным, выявление информационных угроз целесообразно начинать с анализа соответствующих подходов и специфических методов данных воздействий, которые, как правило, осуществляются в рамках информационных (информационно-психологических, психологических) операций.

Отдельно следует отметить роль ТГ-каналов, которые в последнее время стали ключевым инструментом освещения политических процессов, в том числе средством управления социальными группами практически в режиме реального времени. На платформе «Телеграм» западные структуры выстраивают свои самые современные и эффективные, так называемые «сетецентрические» модели управления, противостоять которым в настоящее время практи-

чески невозможно. Анализ наиболее популярных пяти ТГ-каналов показал (по данным сервиса TGStat.ru), что суммарное количество подписчиков только на эти каналы увеличилось за первые 6 месяцев 2020 года более чем в два раза (с 317 128 до 672 310, рис. 3).

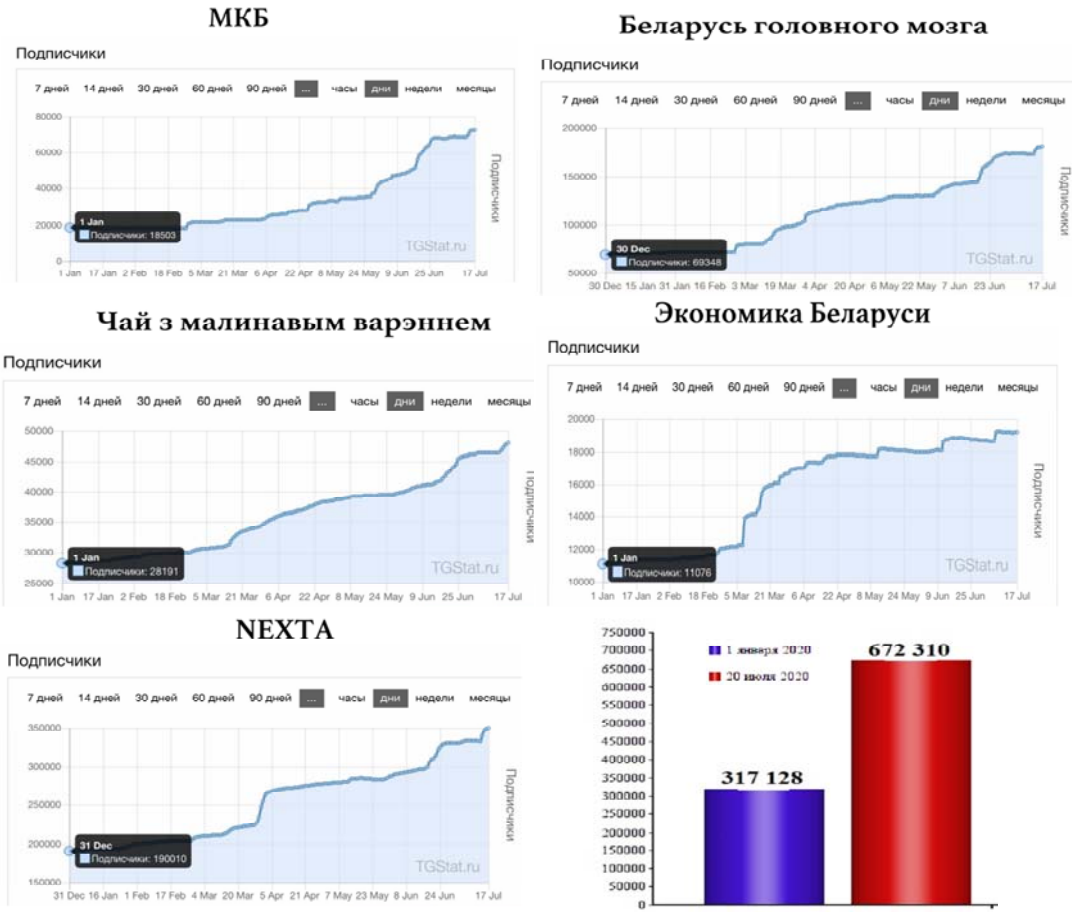


Рис. 3. Рост пользователей наиболее популярных ТГ-каналов в Республике Беларусь за первые 6 месяцев 2020 года

Несмотря на выявленные закономерности, которые имеют практическую (прикладную) направленность, имеются существенные сложности в исследовании процессов изменения эмоциональных состояний больших социальных групп и, соответственно их поведения. Это обусловлено тем, что проблематика исследований относится к слабоструктурированной предметной области, а решение подобных задач связано с целевой, информационной и поведенческой неопределенностями, которые практически не поддаются формальному математическому (аналитическому) описанию рассматриваемых процессов. Это создает определенные трудности в прогнозировании ситуации и принятии рациональных решений.

Таким образом, целенаправленные информационно-психологические воздействия посредством различных СМК ведут к росту негативизации общественного настроения и, как следствие, – росту протестного потенциала. Кроме того, анализ информационного контента, рост пользователей мессенджеров, особенно ТГ-каналов, вовлеченности граждан нашей страны в политический процесс, связанный с выборами Президента республики, позволил констатировать тот факт, что в отношении нашего государства проводится информационная операция, направленная на дестабилизацию общества и смену политического руководства. Это требует разработки соответствующего инструментария, способного выявлять негативизацию эмоциональных состояний БСГ и прогнозировать их поведение.

Список литературы

1. Перова, М. Б. Протестный потенциал России / М. Б. Перова // Научный центр изучения социально-экономических конфликтов. – 2014.

УДК 327.8

ИНФОРМАЦИОННОЕ ПРОСТРАНСТВО КАК ГЕОПОЛИТИЧЕСКАЯ КАТЕГОРИЯ ЭПОХИ ГЛОБАЛЬНОГО МИРА

А.В. ХРОМОВА
Акционерное общество «Перспективный мониторинг», г. Москва, Российская Федерация

Введение. Информационное пространство продолжает оставаться важным фактором становления государства. Как объект исследования представляет особый интерес для международного сотрудничества ввиду растущих угроз по всему миру. Вследствие этого появляются представления об информационной геополитике, об информационной парадигме геополитики, согласно которой «судьба пространственных отношений определяется прежде всего информационным превосходством в виртуальном пространстве» [3]. Стремительное, многовекторное развитие глобального информационного пространства, информационных технологий и коммуникационных систем требует выработки эффективных механизмов противодействия угрозам стратегической стабильности.

Геополитическая роль информационного пространства. Кабанов Ю.А. В своей работе «Информационное пространство как новое (гео)политическое пространство: роль и место государств» выделил следующие типы понимания ИП: синергетическое (автономное поведение – самоорганизация), технологическое (информационно-коммуникационная инфраструктура), социальное (сфера общественно-информационных отношений) и др. [3]. Сегодня наиболее актуальным является социальный тип ИП ввиду наличия массового распространения.

Затруднительность в точном определении термина связана с изменяющимся характером информационного пространства. ИП развивается, мутирует под давлением глобализации и международного положения дел. Сегодня киберпространство является центральным объектом изучения информационного пространства, так как «бумажные» традиционные источники информации уходят на второй план, ввиду быстроразвивающихся информационных технологий. В киберпространство переходят большинство средств массовой информации, государственные реестры, а политическая арена становится виртуальной.

Люди по всему миру стали частью глобальной информационной паутины: они могут свободно общаться, обмениваться информацией, а также исследовать культуру других стран в онлайн режиме. Однако вместе со всеми положительными факторами глобального технологического прогресса существует и резкое возрастание инфогенных угроз в мире. Основой информационного пространства является инфокоммуникационная инфраструктура.

Концепция свободного потока информации воспринимается как еще один механизм для доминирования западных экономик мира. Общество подвергается непреодолимому влиянию американских массовых развлекательных телевизионных программ, правительствам становится все труднее остановить поток этого импорта или разработать конкурирующие местные программы.

Для XXI века характерно формирование инфосферы, на которую сделал акцент Д. Лондсдэйл, введя термин «информационная сила», который встает в один ряд с морским могуществом и сухопутной державой. Говоря о взаимосвязи между технологией и геополитикой, важно помнить, что геополитическая теория часто опиралась на предпосылку, что технология может помочь сформировать геополитический мир. Хэлфорд Маккиндер рассматривал развитие железных дорог как ключ к раскрытию потенциала «хартленда» и тем самым сигнализировал о подъеме континентальных держав за счет морских стран. Поэтому не исключено, что дальнейшее его развитие может иметь значительные последствия для стратегии и геополитики. Однако не следует преувеличивать значение информационной революции. Это может привести к определенной форме технологического детерминизма. Маккиндер избежал этой конкретной ловушки, предположив в своей более поздней работе, что сила хартленда может быть компенсирована коалицией Мидленд-Оушен.

Военное сопротивление всегда являлось дорогостоящим мероприятием, в то время как присутствие в информационном пространстве участника международных отношений от-

крывает большие возможности для влияния как на внутреннюю, так и на внешнюю политику и не требует таких же затрат, как в военной сфере. Стоит понимать, что сила любого суверенного государства прямо зависит от экономического, научного, общественного потенциала, что сопровождается наличием военной силы, задача которой сводится к защите территории государства, граждан государства от любых внешних угроз и с целью поддержки экономической, социальной, политической стабильности государства.

Структура ИП состоит из публичной власти, общества и области их пересечения. Из этого можно сделать вывод, что существуют процессы массового информационного обмена между гражданскими ассоциациями, системой публичной власти и ее органами.

Набирает обороты «цифровая дипломатия» – использование новых технологий для решения дипломатических задач. Многоуровневая работа международных организаций несомненно взаимосвязана. Организации призывают международное сообщество обратить внимание на стремительно развивающиеся информационно-коммуникационные технологии и угрозы, которые они несут в себе.

По официальным данным, американские служащие внешнеполитического ведомства имеют более 100 официальных аккаунтов в социальных сетях: LinkedIn, Facebook, Twitter, Instagram с более чем 1 млн подписчиков на аккаунтах ведомств и 3 млн на аккаунтах служащих на 2020 г. В то время как в России 4,5 млн подписчиков в совокупности, а в Беларуси 40 тыс. подписчиков. Данные цифры говорят о неготовности РФ и РБ вести информационное противоборство.

Согласно данным Cybint, на 2020 год 95% данных утекло из правительственных баз, ИБ-компаний и торговых компаний [6].

Уязвимость информационной инфраструктуры, систем коммуникации может привести к изменению концепции национальной обороны и защиты государства – иными словами – национальная экономика, экономические и гражданские системы могут быть подвержены опасности без прямого использования огневой мощи либо каких-то военных действий.

Согласно исследованию Фонда Общественного Мнения (ФОМ), в российском сегменте сети Интернет 114 млн пользователей. По сравнению с предыдущими годами, количество человек увеличилось на 20 млн [5]. В Беларуси эти же показатели равняются 7,5 млн.

Особенностью информационного оружия является то, что оно используется не только в военной области. Информационное оружие может быть использовано для совершения компьютерных преступлений, хакерских атак, причиняющих ущерб имуществу, а также для достижения своих целей в политике. Стоит отметить, что война в информационном пространстве перестает рассматриваться лишь в терминах «информационно-психологической войны» или «мягкой силы», как «оружие массовых разрушений» (weapons of mass disruption).

Наиболее ярким примером применения информационного оружия в политических и военных целях является конфликт на Украине. В частности, во время проведения референдума за присоединение Крыма к России многие СМИ, группы в социальных сетях активно писали, что так называемые «Вежливые люди» (также «зеленые человечки») заставляли голосовать жителей Украины «под дулом автомата» [4]. Подобные заголовки формировали у жителей отрицательное мнение и являлись косвенным поводом для ненависти ко всем гражданам России, что повлияло на рост агрессивного поведения украинцев в сети по отношению к россиянам. Влияние на когнитивное пространство через социальные сети резко изменило скорость распространения информации, расстояние, на которое она распространяется, и легкость доступа. Платформы социальных сетей очень редко несут ответственность за истории, комментарии, мнения и фотографии, которые они публикуют. Они играют в игру чисел. Ценность платформы социальных сетей измеряется в генерации трафика, который, в свою очередь, создает доход от рекламы, поэтому трафик ускоряется алгоритмами, которые дают потребителям то, что они хотят видеть или слышать. Анализ социальных сетей позволяет политологам понять, что люди смотрят, читают и потребляют. Таким образом, аналитики могут понять общественное мнение и политические пристрастия. Исходя из этого, легко адаптировать кампании к конкретным сообществам, укрепляя существующие убеждения или предрассудки.

Кибератака, направленная на важную государственную инфраструктуру формирует благоприятные условия в отношении развития экстремистских и террористических организаций, координаций действий террористической и экстремистской направленности, что является прямой угрозой национальной безопасности государства (также представляет экономические и политические угрозы, угрозы региональной безопасности) и перетекает уже в другую, не менее серьезную угрозу – кибертерроризм.

Согласно исследованию рынка страхования, Lloyd`s of London пришли к выводу, что скоординированная кибератака способна нанести ущерб экономике в размере от $90 млрд. – $200 млрд. Наибольшие убытки от атак понесут такие сектора как: здравоохранение, банковский и промышленный [6]. Киберпреступления, направленные против критически важной инфраструктуры и государственных объектов нарушают государственный суверенитет и влекут за собой деструктивные последствия для политической и экономической стабильности государства:

1. Вирусу Industrial приписывают причину отключения электроэнергии на Украине в 2016 году.

2. В 2017 году была совершена вирусная атака на системы безопасности нефтехимического завода на Ближнем Востоке. Вирус назывался Triton.

3. В 2018 году вирус с похожими характеристиками на Stuxnet совершил ряд атак на сетевую инфраструктуру Ирана.

Более широкие геополитические и экономические последствия пятого измерения напрямую зависят от того, насколько эффективной может быть информационная власть в стратегическом мире средств и целей. Иногда и в некоторых случаях информационная мощь может оказаться достаточной для достижения политических целей.

Кроме того, информационная революция может усилить мощь обычной военной мощи государства. На самом деле Кеохане и Най идут дальше и правильно отмечают, что географически расположенные национальные государства будут продолжать структурировать политику в информационную эпоху. Однако они могут быть менее точными, когда предполагают, что национальные государства будут больше полагаться на информацию и меньше на материальные ресурсы. Кроме того, Дж. Най в своих трудах ввел термин «мягкой силы», включающий в себя рычаги давления.

Геополитический ландшафт изменится, потому что форма стратегической власти (информационная власть) может быть спроецирована глобально без обращения к физической географии. Однако ограниченность информационной власти, связанная с основным доминированием физической географии, предполагает, что новая геополитическая реальность будет отражать физическую географию по крайней мере в той же мере, в какой она будет отражать инфосферу.

Заключение. Характеризуя же информационное пространство в качестве непосредственной сферы противоборства, необходимо отметить, что большинство существующих систем взаимодействия и передачи информации в различных странах базируются на компьютерных технологиях и различных информационных инфраструктурах и с каждым годом данная возрастающая зависимость от указанных технологий предполагает, что в случае нанесения информационного удара по данным процессам, указанное действие может нарушить либо полностью парализовать основные системы обеспечения передачи информация и обеспечения безопасности того или иного государства, либо целого региона.

Исходя из этого, способность государств действовать в киберпространстве в контексте оборонительных и наступательных действиях, во многом связана с классическими военными возможностями, играющими важную роль для обеспечения безопасности современного государства.

Глобальные сетевые транзитные каналы связи, вычислительные мощности и технологические элементы, работающие на множественные межнациональные задачи, с одной стороны облегчают и ускоряют доступ к данным, интенсифицируют решение задач в интересах общества, помогают повысить результативность социума. С другой стороны, все перечисленное может быть использовано, как распределенная вычислительная глобальная система для достижения доминирования в цифровом пространстве.

Список литературы

1. Кларк, Р. Третья мировая война: какой она будет? / Р. Кларк, Р. Нейк. – СПб., 2017. – С. 182.
2. Маклюен, М. Понимание медиа: внешние расширения человека / М. Маклюен. – М. – Жуковский, 2018. – С. 389.
3. Кабанов, Ю. А. Информационное пространство как новое (гео)политическое пространство: роль и место государств / Ю. А. Кабанов // Сравнительная политика. – 2014. – №4 (17).
4. Порошенко на Генассамблее ООН по Крыму [Электронный ресурс]. – Режим доступа : https://ru.krymr.com/a/news-poroshenko-na-genassamblee-oon-po-krimu/29781257.html. – Дата доступа : 25.04.2021.
5. Фонд Общественного Мнения [Электронный ресурс]. – Режим доступа : https://fom.ru/SMI-i-internet/13999. – Дата доступа : 25.04.2021.
6. Extreme cyber-attack could cost as much as Superstorm Sandy. 17 Jul 2017 [Electronic resource]. – Режим доступа : https://www.lloyds.com/news-and-risk-insight/press-releases/2017/07/cyber-attack-report. – Дата доступа : 25.04.2021.
7. Cyber Security Facts and Stats [Electronic resource]. – Режим доступа : https://www.cybintsolutions.com/cyber-security-facts-stats/
8. Libicki, M. The Emerging Primacy of Information / M. Libicki // Orbis. – 1996. – Vol. 40/2. – P. 261.

ЗАСЕДАНИЕ № 6
ПЕРСПЕКТИВНЫЕ ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 621.38

ГАРМОНИЗАЦИЯ ТРЕБОВАНИЙ ПО ИНФОРМАЦИОННОЙ И ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РАЗЛИЧНЫХ ОБЪЕКТОВ ЗАЩИТЫ

К.А. БОЧКОВ, П.М. БУЙ, Д.В. КОМНАТНЫЙ
Учреждение образования «Белорусский государственный университет транспорта», г. Гомель, Республика Беларусь

Введение. В последнее время наблюдается активное внедрение информационных технологий во все отрасли народного хозяйства. Практически любая сфера жизнедеятельности человека связана с использованием современных инфокоммуникационных систем. Этот процесс как никогда актуализировал вопросы обеспечения информационной безопасности. В соответствии с Концепцией информационной безопасности Республики Беларусь информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [1]. Чаще всего интересами отдельных граждан Республики Беларусь, организаций, общества в целом и, конечно же, государства в информационной сфере является защита информации. Но методы, обеспечивающие информационную безопасность, не в состоянии охватить весь спектр угроз, которые могут быть реализованы против инфокоммуникационных систем в современном мире с его уровнем технологического прогресса. До появления информационных технологий вопросы обеспечения безопасности систем управления стоял не менее остро, но, актуальные для того времени угрозы, смещали вопросы обеспечения их безопасности с информационной в функциональную сферу, которая и стала в последствии источником некоторых методов и подходов, используемых в настоящее время для обеспечения информационной безопасности. Однако все еще открытым остается вопрос о том, насколько в современном мире остаются актуальными вопросы функциональной безопасности и какова их роль в процессе обеспечения безопасности современных инфокоммуникационных систем.

1. Особенности обеспечения информационной и функциональной безопасности. Общие вопросы требований по информационной безопасности сформулированы в СТБ 34.101.1-2014 (IEC 15408-1:2009) «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» [2]. Предметом защиты в этом направлении является сама информаций, а точнее такие ее основные свойства, как конфиденциальность, целостность и доступность. В соответствии с [3], безопасность информации – это состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Функциональная безопасность – это совокупность таких условий функционирования инфокоммуникационной системы, при которых предотвращаются или минимизируются последствия от внешних или внутренних деструктивных воздействий, приводящих к нарушению процесса штатного ее функционирования. Принципы и методы обеспечения функциональной безопасности описаны в базовом ГОСТ Р МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью» [4].

Для подавляющего большинства современных объектов информационных технологий актуальными являются исключительно вопросы информационной безопасности, т. к. задачами этих объектов является хранение, обработка и/или предоставление информации. К таким

объектам можно отнести персональные компьютеры, мобильные устройства пользователей, Internet of Things (IoT) и т. п.

Концепция информационной безопасности Республики Беларусь указывает на то, что повсеместное функционирование объектов транспорта с автоматизированными системами управления ставит в прямую зависимость жизнь и здоровье населения, экологическую и социальную безопасность от их надежности и защищенности [1]. Но безопасность людей, социальной и экологической сферы не является предметом информационной защиты. Методы и средства обеспечивающие исключительно информационную безопасность не в силах решить эти задачи. Особенно это актуально для автоматизированных систем управления ответственными технологическими процессами (АСУ ОТП), которые широко применяются на железнодорожном транспорте.

Основную роль в обеспечении безопасности движения поездов выполняют системы железнодорожной автоматики и телемеханики (СЖАТ). Такие системы в своем составе используют информационную инфраструктуру и на них должны выполнятся мероприятия по обеспечению информационной безопасности. Но в таких системах не информация должна являться главным объектом защиты, а в случае железнодорожного транспорта это в первую очередь обеспечение безопасности движения поездов. Атака на инфокоммуникационные системы и/или на информацию при обнаружении будет заблокирована, но если она не будет обнаружена (например, действия нарушителя будут признаны законными) или будет направлена исключительно на технологический процесс в обход информационной инфраструктуры (например, электромагнитный терроризм), то могут пострадать люди или может быть нанесен вред окружающей среде. Это будет нарушением критериев опасного отказа. В таком случае преобладающими становятся вопросы функциональной безопасности.

Функциональная безопасность – свойство объекта железнодорожного транспорта, связанного с безопасностью, выполнять требуемые функции безопасности при всех предусмотренных условиях в течение заданного периода времени [5].

Для инфокоммуникационных систем железнодорожного транспорта, как, впрочем, и для многих подобных систем других отраслей необходимо обеспечивать как информационную, так и функциональную безопасность. Зачастую, классические методы, обеспечивающие функциональную безопасность и современные методы, обеспечивающие информационную безопасность, частично перекрывают зоны своей ответственности, которая, касается, например, обеспечения доступности и целостности информации и реализуется организационными мероприятиями.

Известный специалист в области функциональной безопасности профессор Скляр В.В. для того, чтобы избежать дублирования требований для таких инфокоммуникационных систем, рекомендует гармонизировать требования по информационной и функциональной безопасности, сформировать общий жизненный цикл, а также увязать процессы управления безопасностью и условия безопасности объекта защиты. Также, по аналогии с функциональной безопасностью, для которой определены уровни полноты безопасности (SIL), определяются пять (от 0 до 4) уровней информационной безопасности (SL) [6]. На рисунке 1 представлена гармонизированная структура требований к информационной и функциональной безопасности объекта защиты [6]. При такой гармонизации требований процессы обеспечения информационной и функциональной безопасности будут происходить параллельно. Причем, исходя из назначения и характеристик объекта защиты в общем жизненном цикле обеспечения информационной и функциональной безопасности определяется приоритет.

Примером подхода, учитывающего вопросы обеспечения как информационной, так и функциональной безопасности, является СТО РЖД 02.049-2014 «Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. Требования к функциональной и информационной безопасности программного обеспечения. Порядок оценки соответствия» [7]. Опыт использования такого совместного подхода описан в статье [8].

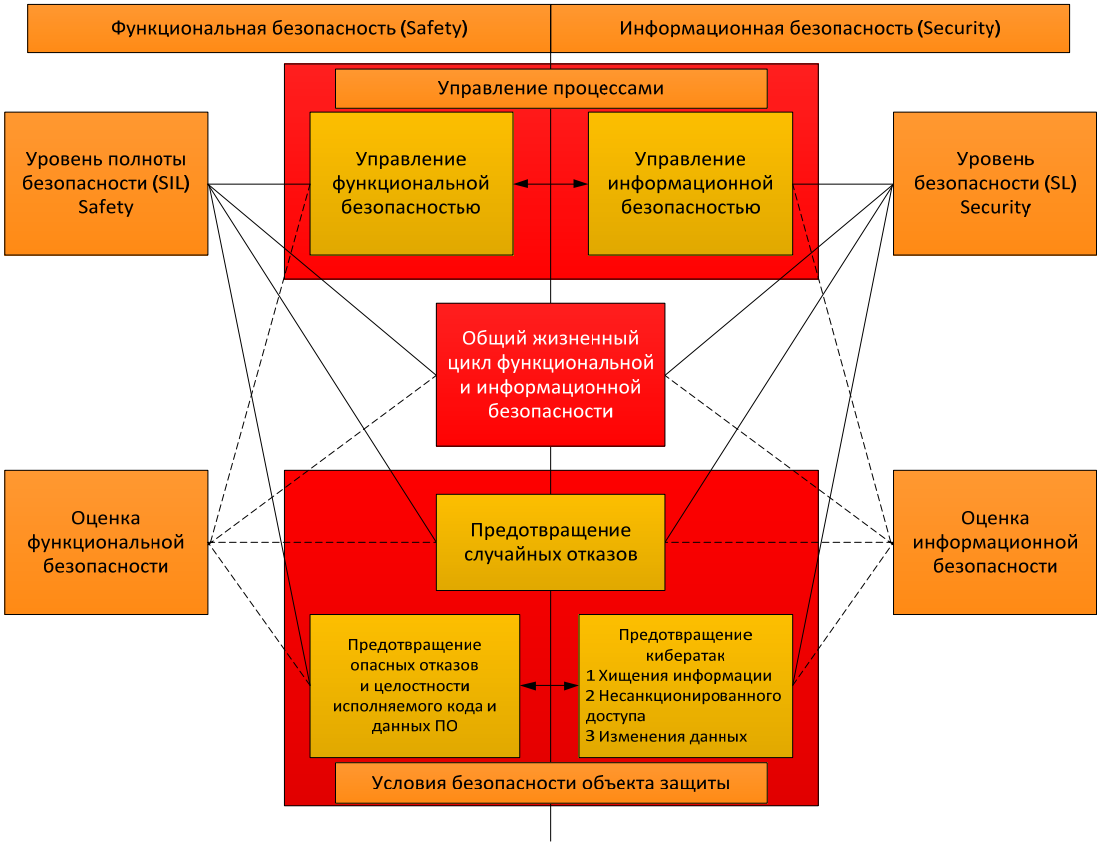


Рис. 1. Гармонизированная структура требований к информационной и функциональной безопасности объекта защиты

2. Безопасность АСУ ОТП железнодорожного транспорта. Уже около десяти лет в Республике Беларусь была выделена особая категория объектов информатизации – критически важные объекты информатизации (КВОИ). Впервые КВОИ упоминается в Указе Президента Республики Беларусь от 9 ноября 2010 г., № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» [9], а в Указе Президента Республики Беларусь от 25.10.2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации», было определено, какие объекты информатизации являются критически важными.

В соответствии с Указом Президента Республики от 09.12.2019 № 449 «О совершенствовании государственного регулирования в области защиты информации» КВОИ – объект информатизации, который на основании критериев отнесения объектов информатизации к критически важным объектам информатизации и показателей уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах включен в Государственный реестр критически важных объектов информатизации [10]. В этом же указе утверждено положение о порядке отнесения объектов информатизации к КВОИ и представлен перечень соответствующих критериев.

Среди критериев отнесения объектов информатизации к КВОИ, указанных в [10], АСУ ОТП железнодорожного транспорта напрямую соответствуют критерию экономической значимости и косвенно могут соответствовать критериям социальной (железнодорожный транспорт является самым дешевым в Республике Беларусь) и экологической (железнодорожный транспорт осуществляет транспортировку опасных грузов, которые могут нанести вред окружающей среде при нарушении безопасности движения поездов) значимости. Однако, насколько известно авторам, ни одна АСУ ОТП железнодорожного транспорта в настоящее время не включена в Государственный реестр КВОИ. В Российской Федерации аналогом КВОИ являются критические системы информационной инфраструктуры (КСИИ) и все СЖАТ, входящие в состав АСУ ОТП, к ним отнесены.

Совокупность угроз информационной и функциональной безопасности потенциально реализуются через кибератаки. Кибератака, в соответствии с [1], – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации. В контексте термина «кибератака» обеспечение информационной и функциональной безопасности можно обозначить термином «кибербезопасность». При таком подходе можно говорить о двухмерной модели кибербезопасности, включающей как информационную, так и функциональную составляющую (рис. 2) [11].

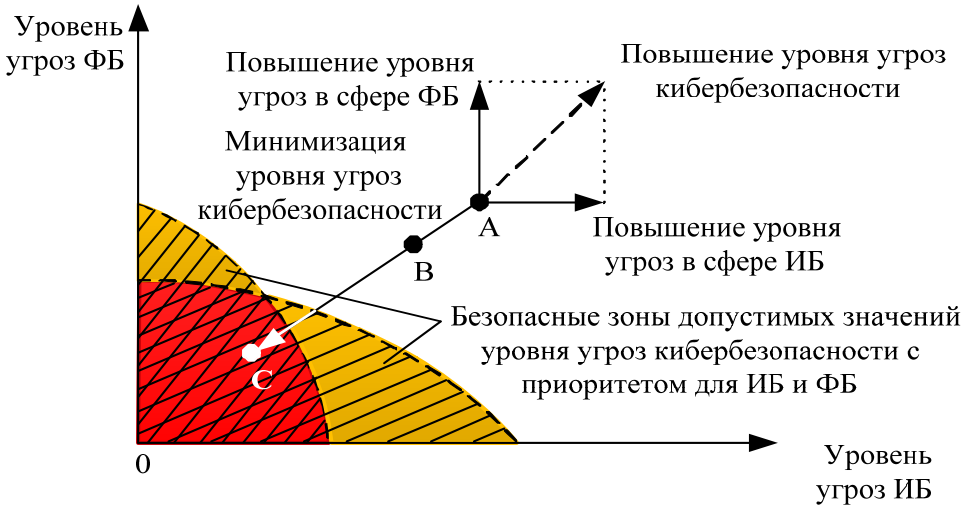


Рис. 2. Двухмерная модель кибербезопасности АСУ ОТП железнодорожного транспорта

Безопасная зона допустимых значений уровня угроз функциональной безопасности дискретно характеризуется уровнем полноты безопасности. Чем выше уровень SIL, тем меньше допускается угроз функциональной безопасности. Аналогичным образом необходимо привязать уровни информационной безопасности к допустимому уровню соответствующих угроз. Точка А, представленная на графике (рис. 2), описывает киберугрозу, при которой нарушается как информационная, так и функциональная безопасность. При необходимости обеспечить требуемые уровни SIL и SL необходимо реализовать такие условия функционирования и использовать средства защиты информации, при которых уровень угроз кибербехопасности будет находится в безопасной зане как по информационно, так и по функциональной безопасности учитывая приоритеты их обеспечения для конкретного объекта защиты (точка С).

Исходя из этой двухмерной модели обеспечение кибербезопасности заключается в соотношении угроз в сферах информационной и функциональной безопасности. При этом, для систем обеспечения безопасности движения поездов, к которым относятся современные микроэлектронные СЖАТ на основе аппаратно-программных комплексов (АПК), преобладающим является обеспечение функциональной безопасности. Кроме того, необходимо учитывать целостность и подлинность технологической информации, циркулирующей в АПК СЖАТ, которая может быть недопустимо искажена при электромагнитных атаках или других видах кибератак.

3. Опасность электромагнитных влияний и терроризма. Одним из новых видов киберугроз АСУ ОТП является «электромагнитный терроризм», суть которого заключается в преднамеренном воздействии на такие системы сверхширокополосными импульсами высокой энергии – электромагнитными импульсами преднамеренного воздействия (ЭИПВ). В связи с этим для обеспечения кибербезопасности АСУ ОТП и, в частности, СЖАТ в современных условиях особое значение приобретает помехоустойчивость. Элементная база таких систем в значительной степени подвержена влиянию электромагнитных помех, а сами СЖАТ работают в сложной электромагнитной обстановке. Не менее актуальной является проблема помехоустойчивости аппаратуры СЖАТ к электростатическому разряду (ЭСР), так как ЭСР обладают сравнимой с ЭИПВ шириной спектра, совпадающего по диапазону с тактовыми частотами ап-

паратуры современных АСУ ОТП. При этом ЭПИВ обладают большей энергией и достаточно трудно локализуемы. Воздействие ЭИПВ или ЭСР может одновременно привести к нарушению как информационной, так и функциональной безопасности.

Анализ последствий такого вида воздействия на АПК СЖАТ осуществляется как для устройств, реализующих алгоритмы безопасности, так и для устройств хранения и передачи информации. Приоритет анализа устанавливается соотношением угроз для информационной и функциональной безопасности АСУ ОТП.

Уровень устойчивости СЖАТ к ЭПИВ и ЭСР, а также их уровень защищенности оцениваются путем расчета и анализа помеховых электромагнитных полей. При этом отличие задачи оценки защищенности СЖАТ от задач электромагнитной совместимости радиоэлектронных средств состоит в том, что ЭПИВ проникают внутрь корпуса-экрана через паразитные (неоднородности корпуса), а не через штатные антенны, как это происходит с узлами радиоэлектронного оборудования. В связи с этим необходимо рассматривать распространение помех внутри корпуса аппаратуры, а не только их прохождение через экран.

Для расчетов электромагнитного поля ЭПИВ могут использоваться численные и аналитические методы. Численные методы основаны на решении интегрального уравнения в частотной области для распределения токов в структуре рецептора [12, 13]:

$$j\omega\frac{\mu}{4\pi}\int\limits_S \vec{J}(r)\frac{\exp(-jkR)}{R}dS - \frac{1}{j4\pi\omega\varepsilon}\int\limits_S \vec{J}(r)\frac{\exp(-jkR)}{R}dS = \vec{E}_t - Z_S\vec{J}(r), \qquad (1)$$

где ω – круговая частота, рад/с;

μ – магнитная проницаемость, Гн/м;

J – плотность тока, А/м^2;

r – радиус-вектор элементарной площадки, м;

k – волновой вектор, рад/м;

R – расстояние между элементарными площадками, м;

S – площадь элементарной площадки, м^2;

ε – диэлектрическая проницаемость среды, Ф/м;

E_t – тангенциальная составляющая помехового электрического поля в пределах элементарной площадки, В/м;

Z_s – полное сопротивление элементарной площадки, Ом.

Аналитические методы позволяют получить пессимистическую, то есть перекрывающую все резонансы в корпусе, оценку помехового поля внутри корпуса рецептора. Они основаны на замкнутых выражениях для электрической составляющей электромагнитного излучения простых излучателей [14–16]. Такая оценка зачастую достаточна для решения задачи оценки уровня защищенности.

Для прямоугольного отверстия в неоднородности корпуса оборудования электрические составляющие поля в сферической системе координат имеют следующий вид:

$$\begin{aligned} E_\Theta &= \frac{jabE(j\omega)}{2\lambda}\frac{e^{-\lambda kR}}{R}(1+\cos\phi)\cos\phi\frac{\sin(0.5ka\sin\Theta\sin\phi)}{0.5ka\sin\Theta\sin\phi}\frac{\sin(0.5kb\sin\Theta\cos\phi)}{0.5kb\sin\Theta\cos\phi}, \\ E_\phi &= \frac{-jabE(j\omega)}{2\lambda}\frac{e^{-\lambda kR}}{R}(1+\cos\phi)\sin\phi\frac{\sin(0.5ka\sin\Theta\sin\phi)}{0.5ka\sin\Theta\sin\phi}\frac{\sin(0.5kb\sin\Theta\cos\phi)}{0.5kb\sin\Theta\cos\phi}, \end{aligned} \qquad (2)$$

где $E(j\omega)$ – напряженность электрической составляющей поля в раскрыве отверстия, В/м;

a, b – стороны отверстия, м;

λ – длина волны, м;

θ, φ – сферические координаты, рад.

Электрические составляющие излучения круглого отверстия в неоднородности корпуса оборудования в сферической системе координат описывается выражениями:

$$E_{\Theta} = \pi r_0^2 \frac{E(j\omega)}{2\lambda R} e^{-jkR}(1+\cos\Theta)\cos\phi,$$
$$E_{\phi} = \pi r_0^2 \frac{-jE(j\omega)}{2\lambda R} e^{-jkR}(1+\cos\Theta)\sin\phi, \quad (3)$$

где r_0 – радиус отверстия, м.

При воздействии как ЭПИВ, так и ЭСР, в раскрыве паразитной антенны создается напряженность поля. В первом случае источником является аппаратура террориста, во втором, – генератор ЭСР, подключенный к паразитной антенне. Сходство каналов проникновения и методов расчета позволяет разработать методику комплексной оценки защищенности СЖАТ от ЭИПВ. Такая методика основывается на сопоставлении воздействия от ЭИПВ и ЭСР на паразитные антенны, а также влияния этого воздействия на кибербезопасность СЖАТ. Методика позволяет косвенно судить о защищенности СЖАТ от ЭИПВ по результатам анализа и испытания защищенности СЖАТ от ЭСР. Такая оценка целесообразна, так как испытания на ЭСР являются обязательными, а оборудование для испытаний доступно и безопасно.

Заключение

1. В НИЛ «Безопасность и электромагнитная совместимость технических средств» Белорусского государственного университета транспорта отработаны технологии, позволяющие прогнозировать поведение АСУ ОТП и, в частности, СЖАТ при воздействии на них ЭПИВ. Испытания проводятся путем принципа эквивалентности с применением стандартных программ тестирования на устойчивость к электростатическим разрядам.

2. Разработана методика оценки соответствия объекта защиты требованиям функциональной и информационной безопасности в соответствии с требованиями с СТО РЖД 02.049-2014 «Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. Требования к функциональной и информационной безопасности программного обеспечения. Порядок оценки соответствия».

3. Проведенные исследования позволяют минимизировать последствия воздействия кибератак за счет дополнения СЖАТ системой поддержки принятия решений (СППР) в нештатных ситуациях.

Список литературы

1. О Концепции информационной безопасности Республики Беларусь : Пост. Совета безопасности Респ. Беларусь, 18 марта 2019 г., № 1 // ЭТАЛОН Законодательство Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.

2. СТБ 34.101.1-2014. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1: Введение и общая модель. – Взамен СТБ 34.101.1-2004 ; введ. 2014–09–01. – Мн. : БелГИСС, 2014. – 60 с.

3. СТБ ISO/IEC 27001-2016 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

4. ГОСТ Р МЭК 61508-3-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению.

5. ГОСТ 33432-2015 Безопасность функциональная. Политика, программа обеспечения безопасности. Доказательство безопасности объектов железнодорожного транспорта.

6. Скляр, В. В. Обеспечение безопасности АСУТП в соответствии с современными стандартами : метод. пособие / В. В. Скляр. – М. : Инфра-Инженерия, 2018. – 384 с.

7. СТО РЖД 02.049-2014 «Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. Требования к функциональной и информационной безопасности программного обеспечения. Порядок оценки соответствия» от 30.12.2014.

8. Бочков, К. А. Особенности обеспечения функциональной и информационной безопасности микроэлектронных систем управления движением поездов на железнодорожном транспорте / К. А. Бочков, Д. В. Комнатный, С. Н. Харлап // Комплексная защита информации : мат-лы XXV Междунар. науч.-практ. конф., Москва, 15–17 сентября 2020 г. – М. : Медиа Групп «Авангард», 2020. – С. 88–95.

9. О совершенствовании государственного регулирования в области защиты информации : Указ Президента Респ. Беларусь от 09.12.2019 № 449 // Эталон Online [Электронный ресурс] / Нац. Центр правовой информации Респ. Беларусь. – Минск, 2020.

10. Об утверждении Концепции национальной безопасности Республики Беларусь : Указ Президента Респ. Беларусь, 09 ноября 2010 года, № 575 с изм. и доп. от 24 января 2014 г. № 49 // Эталон Online [Электронный ресурс] / Национальный Центр правовой информации Республики Беларусь. – Минск, 2018.

11. Бочков, К. А. Кибербезопасность автоматизированных систем управления ответственными технологическими процессами железнодорожного транспорта / К. А. Бочков, П. М. Буй // Проблемы безопасности на транспорте : мат-лы X Междунар. науч.-практ. конф., Гомель, 26–27 ноября 2020 г. / Бел. гос. ун-т трансп.; редкол. : Ю. И. Кулаженко [и др.]. – Гомель : БелГУТ, 2020. – С. 7–9.

12. Михайлов, В. А. Разработка методов и моделей анализа и оценки устойчивости функционирования бортовых цифровых вычислительных комплексов в условиях преднамеренного воздействия сверхкоротких электромагнитных излучений : автореф. дис. … д-ра техн. наук / НИУ ВШЭ. – М., 2014. – 45 с.

13. Акбашев, Б. Б. Теоретические и экспериментальные методы оценки устойчивости терминалов к воздействию сверхширокополосных электромагнитных импульсов : дис. … канд. техн. наук: 05.12.13 / Б. Б. Акбашев. – М., 2005. – 156 с.

14. Иванов, В. А. Электромагнитная совместимость радиоэлектронных средств / В. А. Иванов, Л. Я. Ильницкий, М. И. Фузик. – Киев : Техника, 1983. – 189 с.

15. Модель дифракции высокочастотной электромагнитной волны на апертуре в проводящем экране / Д. А. Ционенко [и др.] // Доклады БГУИР. – 2015. – № 5. – С. 5–11.

16. Бочков, К. А. Элементы моделирования электромагнитной совместимости устройств железнодорожной автоматики и телемеханики / К. А. Бочков, Д. В. Комнатный. – Гомель : БелГУТ, 2013. – 185 с.

УДК 343.985

ПАССИВНАЯ ИНТЕРНЕТ-РАЗВЕДКА НА ОСНОВЕ ОТКРЫТЫХ ИСТОЧНИКОВ (OSINT) В СОВРЕМЕННЫХ УСЛОВИЯХ: СУЩНОСТЬ, МЕТОДОЛОГИЯ, ОБЗОР ИНСТРУМЕНТАРИЯ

П.Л. БОРОВИК
Учреждение образования «Академия Министерства внутренних дел Республики Беларусь», г. Минск, Республика Беларусь

В соответствии с абзацем 2 ст. 3, п. 1 ч. 1 ст. 7 Закона Республики Беларусь от 15.07.2015 № 307-З «Об оперативно-розыскной деятельности» и п. 4 ч. 2 ст. 37 УПК Республики Беларусь сотрудники оперативных подразделений органов внутренних дел проводят необходимые оперативно-розыскные мероприятия и принимают иные меры в целях обнаружения преступлений, и выявления лиц, их совершивших. Проводимые ими оперативно-розыскные мероприятия и иные меры могут быть направлены, в первую очередь, на сбор и анализ информации из открытых источников сети Интернет с целью выявления конкретных пользователей глобальной сети, которые причастны к их совершению.

Поисковые мероприятия в сети Интернет фактически представляют собой поиск, сбор и анализ сведений из открытых источников с использованием подручных средств. Такой вид деятельности принято называть одним из направлений OSINT (от англ. *Open Source Intelligence*) – разведка на основе открытых источников, суть которой заключается в поиске, сборе и анализе информации. В данном случае под открытыми источниками понимаются общедоступные ресурсы в сети Интернет, к которым относятся интернет-сообщества, блоги и форумы, социальные сети и популярные «мессенджеры» (программы мгновенного обмена сообщениями), видео-хостинги и файлообменные серверы.

Существует два типа интернет-разведки: пассивная разведка на основе открытых источников и активная разведка с применением вредоносных атак. В контексте рассматриваемой проблематики, а также с учетом решаемых задач практический интерес представляет *пассивная интернет-разведка*, под которой обычно понимается первоначальный сбор общедоступной информации из открытых сетевых ресурсов об объекте. Утилитарная значимость данной разновидности OSINT обусловлена тем, что с ее помощью можно достаточно эффективно и в кратчайшие сроки подобрать соответствующий комплекс дальнейших оперативно-розыскных мероприятий, методов и средств, позволяющих установить всех участников преступной группы, выяснить роль каждого из фигурантов, а также иные обстоятельства, свидетельствующие об их преступной деятельности.

Процесс осуществления пассивной интернет-разведки условно можно разделить на следующие этапы: определение объектов поисковых мероприятий, конкретизация целей (определение конкретных установленных или неустановленных лиц; групп лиц, объединенных общими признаками; событий и их обстоятельств, представляющих интерес; интернет-ресурсов, в отношении которых планируется сбор информации); определение инструментов, методов и средств, с помощью которых будут осуществляться поисковые мероприятия; непосредственно поиск и сбор информации; анализ полученной информации, документальное оформление.

Поиск может осуществляться как традиционными поисковыми системами (например, «Google», «Yandex»), так и с использованием поисковых функций целевых форумов, социальных сетей и иных онлайн-ресурсов.

Наиболее часто используемыми и универсальными инструментами являются поисковые системы «Google», «Yandex», «Rambler.ru», «Yahoo.com», «Bing.com», «Duckduck.go» и др. Благодаря сохранению копий поисковыми системами в ряде случаев можно получить доступ к интересующей информации, даже если оригиналы интернет-страниц заблокированы или удалены.

Альтернативным, но не менее эффективным поисковым инструментом являются метапоисковые машины – поисковые системы, которые в отличие от классических поисковых машин не имеет собственной базы данных и собственного поискового индекса, а формирует

поисковую выдачу за счет смешивания и переранжирования результатов поиска других поисковых систем. Наиболее популярными среди них являются следующие: «eTools» (*www.etools.ch/search.do*), «eLocalFinder» (*www.elocalfinder.com/HSearch.aspx*), «Search» (*https://www.search.com*) и др.

В ходе осуществления OSYNT целесообразно использовать поисковые системы, ориентированные на конфиденциальность пользователя (не отслеживающие действия, запросы, IP-адрес, сведения об установленной операционной системе и пр.): «DuckDuckGo» (*https://duckduckgo.com/*); «Oscobo» (*https://oscobo.co.uk*); «Swisscows» (*https://swisscows.com*); «Gigablast» (*https://www.gigablast.com*) и др.

Иногда аналитику необходимо вернуться назад во времени, чтобы исследовать содержимое какого-либо web-сайта в прошлом. В этом случае рекомендуется воспользоваться специальными сетевыми сервисами, например, «Архив Интернета» (*http://web.archive.org/*). Система сохранят состояние страниц, доступных под интересующими доменными именами, актуальное на некоторую дату, благодаря чему аналитик может получить представление об искомом сайте, и в некоторых случаях историю развития ресурса с момента его попадания в базу сервиса. Данный сервис позволяет сохранять текущие состояние интернет-страниц для их последующего использования, а также делает «скриншот» (снимок экрана), содержащий сохраняемую страницу.

Альтернативными ресурсами, позволяющими осуществлять поиск архивных копий сайтов, являются «Веб-архив» (*http://web-arhive.ru/*) и «Achive.Today» (*https://archive.vn/*).

В ряде случаев аналитику может понадобиться информация об изменениях на определенном веб-сайте. Отслеживание изменений на одном веб-сайте может быть достигнуто путем регулярного его посещения. Однако, как быть, если необходимо осуществить отслеживание изменения страниц на многих сайтах одновременно?

Для решения данной задачи рекомендуется использовать сервисы мониторинга веб-сайтов, позволяющие отслеживать неограниченное количество страниц, в том числе с автоматическим оповещением по электронной почте. Наиболее распространенными среди них являются: «Google Alerts» (*https://www.google.com/alerts*), «Talk Walker» (*www.talkwalker.com/alerts*), «Visual Ping» (*https://visualping.io*), «Update Scanner» (*https://addons.mozilla.org/en-US/firefox/*) и др.

Отдельно следует остановиться на поиске информации в анонимной сети «Tor». Примерами поисковых систем в такой сети являются «Oneirum» (*http://oneirunda366dmfm.onion*), «not EVIL» (*http://hss3uro2hsxfogfq.onion/*), «Candle» (*http://gjobqjj7wyczbqie.onion/*), «Torch» (*http://xmh57jrzrnw6insl. onion/*) и др.

Несмотря на то, IP-адреса сайтов в сети «Tor» зашифрованы, существуют технологии, позволяющие деанонимизировать пользователей такой сети. Наглядным примером реализации указанной возможности является онлайн-сервис «Darktracer.io» (*https://darktracer.io/*), который выполняет сканирование в сети «Tor», обнаруживает реальные адреса IPv4 (IPv6) onion-сайтов и заносит их в свою базу данных.

Отдельно следует остановиться на возможностях поиска информации о конкретных лицах в сети «Интернет». Так, существуют онлайн-сервисы, с помощью которых можно удобно и быстро находить размещенные в открытом доступе профили людей в социальных сетях. Для поиска не требуется регистрация в социальных сетях (хотя она может потребоваться, если вам нужно связаться с человеком, которого вы нашли). Например, традиционный поисковый сервис «Яндекс» (https://yandex.by) умеет группировать профили, принадлежащие одному и тому же человеку. Благодаря этому поиск упрощается: на выдаче по запросу помещается больше результатов, и пользователь может выбрать, в какой социальной сети ему удобнее общаться с найденным человеком.

Существуют и специализированные сервисы для поиска аккаунтов социальных сетей. Например, онлайн-сервис «Найти человека» (*https://poisk-cheloveka.ru*) собирает информацию о людях из открытых баз данных интернета, а для осуществления поиска используются данные из открытых источников, включая такие социальные сети, как «ВКонтакте», «Одноклассники», «Facebook» и «Twitter». Подобными возможностями обладает и альтернативный сетевой ресурс от «Mail.ru» (*https://go.mail.ru/search_social*).

Эффективным средством поиска в социальной сети «ВКонтакте» представляется сетевой сервис «220vk» (*https://220vk.com*). Помимо наличия расширенных поисковых возможно-

стей он позволяет определять: добавление либо удаление друзей и подписчиков; подписки либо отписки на сообщества; изменения имени, фамилии, адреса страницы, города, даты рождения и семейного положения др.

Поиск людей можно также осуществлять непосредственно на сайтах социальных сетей по имеющейся исходной информации (обычно имя и фамилия, возможно использование вымышленных никнеймов), для конкретизации поиска используется фильтрация по региону, возрасту и другим параметрам.

Важное значение при осуществлении поисковых мероприятий в сети «Интернет» имеет поиск по заданному изображению (цифровой фотопортрет, аватар, рисунок, фрагменты фото и пр.), а также идентификация лица, изображенного на ней. Для этих целей рекомендуется использовать следующие онлайн-сервисы: «Яндекс-картинки» (*https://yandex.ru/images/*); «Google – images» (*https://images.google.com/*); «Mail.ru – images» (*https://go.mail.ru/search_images*); «Tineye» (*https://tineye.com/*).

Возможны поиск по фотографии и соответствующая идентификация в социальных сетях с использованием следующих онлайн-ресурсов: «FindClone» (*https://findclone.ru/*), «Search4faces» (*https://search4faces.com/*).

В случае, если исходное качество фотографии, которую планируется использовать для поиска в сети, является неудовлетворительным, его можно повысить, используя специализированные сетевые сервисы: «Let`enhance» (*https://letsenhance.io/*), «Pinkmirror» (*https://pinkmirror.com/*), «Improvephoto» (*https://improvephoto.net/*) и др.

Обнаружить следы фотомонтажа на фотографии можно, используя следующие сетевые инструменты: «Forensically» (*https://29a.ch/photo-forensics/#error-level-analysis*), «ImageEdited» (*http://imageedited.com*) и др.

Для того, чтобы просмотреть метаданные имеющейся фотографии (метаданные фотографии или EXIF – стандарт, позволяющий добавлять к изображениям и прочим медиафайлам дополнительную информацию, комментирующую этот файл, описывающий условия и способы его получения, авторство, дата и время съемки, GPS-координаты и т. п.), рекомендуется использовать возможности такиех онлайн-ресурсов, как «Jeffrey's Image Metadata Viewer» (*http://exif.regex.info/exif.cgi*), «IMGonline» (*https://www.imgonline.com.ua/*), «Pic2map» (*https://www.pic2map.com/*), «Fotoforensics» (*http://fotoforensics.com/*).

Распознать объекты, изображенные на имеющейся фотографии (например, растения, предметы, архитектурные объекты, сооружения и др.) помогут специальные онлайн-ресурсы: «Merlin» (*https://merlin.allaboutbirds.org/*), «Pl@ntNet» (*https://identify.plantnet.org/*), «Яндекс-картинки» (*https://yandex.ru/images/*), «Google-картинки» (*https://images.google.com/*) и др.

В ходе анализа фотографии аналитик может установить примерное время фотосъемки (при отсутствии указанных данных в EXIF). Для этого ему следует воспользоваться специализированным онлайн-сервисом определения времени по солнцу «Suncalc» (*https://www.suncalc.org/*).

При необходимости оценки количества запечатленных на фотографии людей, расположенных на некоторой территории (участке, площади и пр.), рекомендуется обратиться к специализированному сетевому ресурсу «Mapchecking» (*https://www.mapchecking.com/*).

Следует отметить, что в сети «Интернет» существуют специализированные сервисы, позволяющие получить исчерпывающую информацию о цифровом изображении. Так, на онлайн-ресурсе «Osint Photo» (*https://start.me/p/0PgzqO/osint-photo*) представлены десятки полезных инструментов: от просмотра метаданных до идентификации объектов на фото. Сервисы разбиты на категории, среди которых: сайты по распознаванию лиц, обратному поиску фото, определению оригинальности, качества и возраста лица на фото и др.

В контексте рассматриваемой темы важное практические значение имеет поиск и комплексный анализ информации в социальных сетях, в том числе с использованием специализированных аналитических и вспомогательных интернет-сервисов (например, «VK LikeChecker» (*https://vk.com/app3429542*), «ZebraBoss» (*https://ru.zebraboss.com/*), «ВК-шпион» (*http://vk.city4me.com/*), «Барков.Нет» (*https://vk.barkov.net/*) и др.). Это поможет составить психологический портрет владельца сетевого ресурса и с достаточно высокой степенью достоверности определить его текущие настроения, а также спрогнозировать некоторые его действия.

Любая современная социальная сеть предлагает, как правило, базовый, минимальный набор сервисных услуг: хранение персональных установочных данных (без предоставления которых невозможна регистрация в сети), виртуальный органайзер, некая совокупность мультимедийных данных пользователя (фото- и видеоматериалы, музыка) и некоторые другие персональные информационные блоки. Используя эти данные, можно выстроить персональный психологический профиль владельца страницы, включающий в себя следующие составляющие: персональные установочные данные (возраст, место рождения и проживания, образование, национальность и т. д.); преобладающий тип темперамента, доминирующие настроения индивида (анализируя содержание новостной ленты страницы, музыкальные предпочтения, личные фотографии); основные черты характера личности (так называемые акцентуации); коммуникативные особенности, социальную активность личности, ее потребностно-мотивационную сферу (комплексный анализ содержания персональной страницы, включая участие в деятельности различных виртуальных групп, подразделяющихся по гендерным, возрастным, профессиональным признакам, интересам и предпочтениям); социальные связи субъекта (используя графический, узловой метод анализа). Особое внимание при анализе страниц следует уделить статусу владельца страницы и по возможности выявить частоту его изменения.

При анализе персональной страницы, безусловно, следует принимать во внимание тот факт, что некоторые люди при регистрации аккаунтов не указывают свои реальные биографические данные (например, год рождения или место проживания). В этом случае имеется возможность получить требуемую информацию, используя параметры профилей наиболее близких друзей. Например, город проживания пользователя можно установить на основе анализа его подписок, постов и статусов.

Кроме данных, которые пользователи сети указывают в своих профилях, многое можно узнать, анализируя посты, группы подписки и фотографии. При этом с точки зрения психологии интерес представляют дополнительные факты, которые можно извлечь из этой неструктурированной информации. Определенный интерес представляют сообщения и тексты, написанные самим владельцем страницы. Способ лингвистического анализа текста (лексика, стилистика, наличие жаргонизмов, набор фраз) позволяет определить принадлежность индивида к определенной социальной, возрастной и гендерной группе и многое другое. С этой целью формируется набор текстов пользователей с известными установочными данными, выявляются особенности текстов для каждой группы и формируется некоторая формальная модель, позволяющая оценить принадлежность автора к определенной группе.

Мероприятия по сбору и анализу содержащейся в социальных сетях Интернета информации о лицах состоят из следующих этапов: установление факта регистрации лица в социальной сети, определение веб-адреса его персональной страницы; анализ содержания персональной страницы лица; выявление, визуализация и анализ связей лица с другими пользователями социальной сети.

Так, для установления факта регистрации лица в социальной сети и определения веб-адреса его персональной страницы целесообразно использовать возможности поисковых систем (например, «Яндекс»), рассмотренных нами ранее.

Если оригинал персональной страницы лица не доступен (он может быть удален либо поисковая система считает его потенциально опасным), существует возможность просмотра его последней сохраненной (кэшированной) копии. Для этого следует нажать на кнопку «перейти по ссылке «Сохраненная копия”« рядом с адресом документа, позволяющую перейти к сохраненной копии страницы.

В случае, если индексация профиля запрещена владельцем аккаунта социальной сети, либо он зарегистрировался в сети менее двух недель назад, поиск его персональных страниц необходимо осуществлять в каждой социальной сети отдельно.

Анализ содержания персональной страницы лица в социальной сети предполагает изучение следующих основных элементов персональной страницы лица (на примере социальной сети «ВКонтакте»): аватар, статус пользователя, друзья, информация о пользователе, лайки, сообщения, комментарии, музыка, видео, группы (сообщества), приватность страницы.

Выявление, визуализация и анализ связей лица с другими пользователями социальной сети предполагает использование возможностей специализированного интернет-сервиса визуализации связей «Yasiv» (*https://www.yasiv.com/vk*). С его помощью можно наглядно, в виде интерактивного графа (диаграммы связей), установить взаимосвязи пользователей социальной сети «ВКонтакте» как по отношению к искомому лицу, так и друг с другом.

Выявленную в ходе сетевой разведки информацию рекомендуется фиксировать прямо в процессе поиска созданием «скриншотов» (графических отображений экрана), содержащих, по возможности, не только сами сведения, но и электронный адрес ресурса их размещения, дату публикации, прочие сопутствующие сведения. Полученные в ходе поиска данные могут быть записаны на компакт-диск или выведены на печать (в зависимости от объемов и качества полученной информации) и приобщены к протоколу проведенного мероприятия или следственного действия в виде несекретного приложения.

Дальнейшие действия по установлению сведений о лицах, причастных к совершению конкретных правонарушений, связаны с применением всего комплекса оперативно-розыскных сил, средств и методов, подтвердивших свою эффективность в противодействии общеуголовной преступности. При выявлении указанной категории лиц их действия также необходимо контролировать с целью последующего использования полученной оперативной информации для документирования и расследования соответствующей преступной деятельности.

УДК 629.01; 621.3.019.3

ОСОБЕННОСТИ ОПТИМИЗАЦИИ ПОДСИСТЕМ ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ НАВИГАЦИОННО-ИНФОРМАЦИОННЫХ СИСТЕМ

А.Н. КОРОЛЕВ, Г.В. КОРОВИН
«НИИ КС им. А.А. Максимова» – филиал АО «ГКНПЦ им. М.В. Хруничева», г. Королев, Российская Федерация

Введение. На современном этапе развития техники практически любая система управления подвижными объектами представляет собой автоматизированную информационную систему, предназначенную для обработки пространственно-временных и иных данных об объектах управления, основой которой служит навигационная и телеметрическая информация о их состоянии. Широкий класс таких систем объединяет общее название – навигационно-информационные системы (НИС).

Основной особенностью НИС по сравнению с другими информационно-управляющими системами является то, что источником деструктивных воздействий, вызывающих аппаратные, программные, информационные отказы и отказы по вине персонала, приводящие, в свою очередь, к снижению надежности и безопасности функционирования системы, помимо внешней среды и внутреннего состояния системы выступает пространственно-временная конфигурация НИС. Вследствие неоднородности навигационных и связных полей взаимное пространственно-временное расположение подвижных объектов и органов (пунктов) управления ими может вызывать дополнительные информационные отказы, связанные со снижением качества навигационной информации и задержками или потерями информации при передаче ее между объектами системы.

В связи с этим эффективность функционирования НИС полностью зависит от ее функциональной устойчивости, то есть способности сохранять или восстанавливать (полностью или частично) возможность выполнения возложенных на нее функций в условиях деструктивных воздействий [1]. Такая способность обеспечивается введением в состав НИС специальной подсистемы обеспечения функциональной устойчивости (ПОФУ). Однако наличие в составе НИС подсистемы обеспечения функциональной устойчивости не только обеспечивает качество функционирования НИС на требуемом уровне, но и влечет за собой дополнительные затраты. Очевидно, что для повышения эффективности НИС необходимо, чтобы приращение в качестве функционирования вследствие реализации функциональной устойчивости превышало приращение в затратах на создание и эксплуатацию ПОФУ, то есть создание ПОФУ представляет собой сложную оптимизационную задачу, решение которой зависит от многих факторов.

1. Общая постановка задачи синтеза подсистемы обеспечения функциональной устойчивости НИС и методология ее решения.

Под архитектурой ПОФУ НИС будем понимать совокупность методов и средства обеспечения функциональной устойчивости НИС и способов информационного взаимодействия между ними.

Задача синтеза архитектуры ПОФУ относится к классу задач принятия системотехнических решений в рамках общей теории выбора [2, 3]. В соответствии с общей моделью принятия решений [4] формально постановку задачу синтеза архитектуры НИС можно определить следующим образом.

Определены множества вариантов структурного построения НИС, компонентов и комплексов программного, технического и информационного обеспечений, методов и средств обеспечения функциональной устойчивости, а также способов информационного взаимодействия между ними, на основе которых может быть сформировано множество проектных решений (альтернативных архитектур ПОФУ), множество критериев и шкал их измерений, а также тип принимаемого решения, определяемый видом структуры множества альтерна-

тив. Требуется выбрать альтернативы на этом множестве в соответствии со определенной его структурой.

Для выбора проектного решения необходимо построить решающее правило, которое позволяло бы упорядочить множество альтернатив в соответствии с принятой структурой.

Синтез архитектуры ПОФУ будем рассматривать как процесс определения совокупности подсистем контроля, планирования и реконфигурации ресурсов системы, обеспечивающих максимально возможный уровень качества реализации функций НИС при известной модели угроз деструктивных воздействий на систему.

Архитектуру ПОФУ h_{φ}^{st} из множества возможных архитектур H^{st} будем называть *эффективным решением* (эффективной архитектурой) в соответствии с решающим правилом R, если не существует такого элемента $h_{\chi}^{\text{st}} \in H^{st}$, для которого выполняется отношение $h_{\chi}^{\text{st}} R h_{\varphi}^{st}$. Другими словами, эффективным называется такое решение h_{φ}^{st}, которое нельзя улучшить по какому-нибудь одному из компонент векторного критерия W, не ухудшив при этом хотя бы один из остальных компонент этого критерия.

Задача синтеза может быть декомпозирована в соответствии с применяемыми решающими правилами:

1) Задача синтеза на основе некоторого отношения предпочтения R, обеспечивающего выбор подмножества эффективных архитектур $P(H^{st})$ в соответствии с векторным критерием W;

2) Задача синтеза на основе отношения предпочтения $\hat{R}$, обеспечивающего выбор рациональной архитектуры в соответствии с обобщенным критерием $Q(W)$.

Первая задача решается на начальных этапах создания ПОФУ при определении перспективных вариантов архитектур ПОФУ для создаваемой НИС. Вторая – на этапах принятия окончательного технического решения по облику ПОФУ.

Следовательно, решение задачи синтеза архитектуры ПОФУ функционально устойчивой НИС состоит из двух этапов (рис. 1).

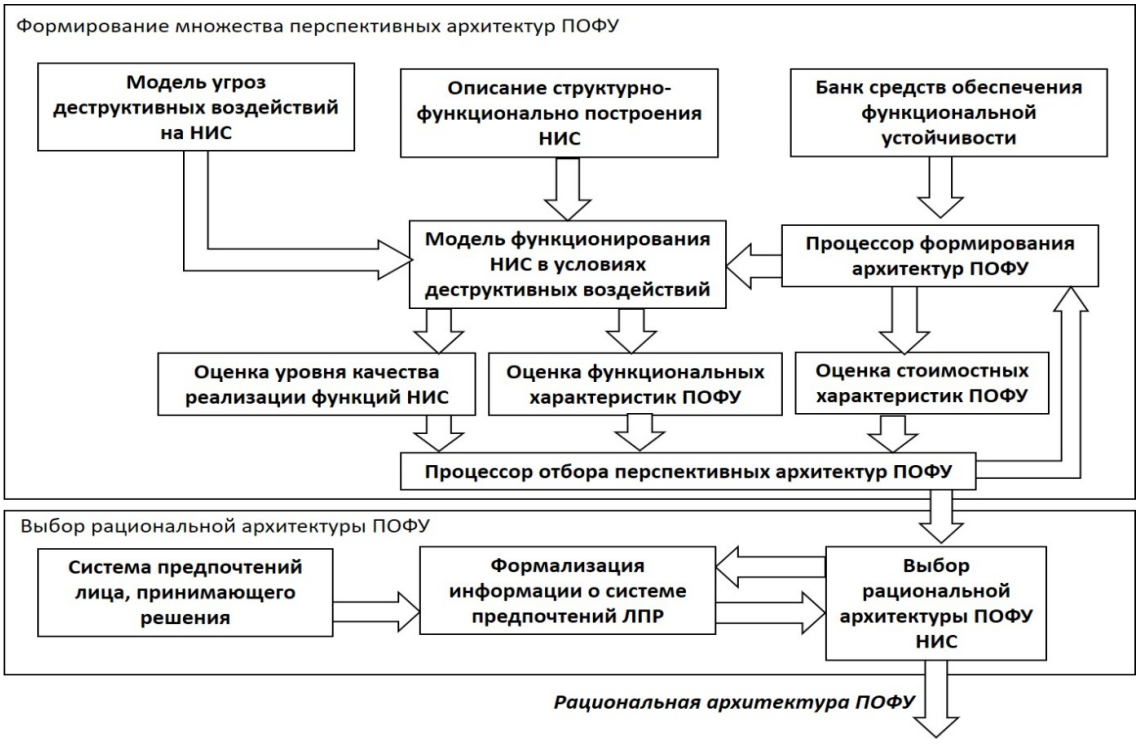


Рис. 1. Общая схема решения задачи синтеза рациональной архитектуры ПОФУ НИС

На первом этапе осуществляется формирование множества Парето $P(H^{st})$ эффективных архитектур ПОФУ на множестве H^{st}.

Второй этап представляет собой собственно процедуру выбора рационального варианта h_*^{st} на множестве $P(H^{st})$ в соответствии с $Q(W)$.

Для решения данной задачи необходимо:

1. Построить множество эффективных вариантов архитектур ПОФУ. Для чего:

1.1. Сформировать множество возможных вариантов архитектур ПОФУ $\dot{H}^{st}$.

1.2. Из множества $\dot{H}^{st}$ сформировать множество допустимых вариантов архитектур ПОФУ $\dot{H}^{st}$ путем проверки выполнения ограничений.

1.3. Из множества $\dot{H}^{st}$ построить множество эффективных (Парето-оптимальных решений) $P(H^{st})$ путем попарного сравнения элементов множества H^{st} по элементам W_1, …, W_n векторного критерия W.

2. Определить рациональный вариант h_*^{st} архитектуры ПОФУ на множестве $P(H^{st})$ с использованием вектора предпочтений $\boldsymbol{\alpha}$

$$h_*^{st} = \arg\operatorname{ext} Q(\alpha, W(h_i^{st})).$$

2. Особенности выбора рациональной архитектуры подсистемы обеспечения функциональной устойчивости НИС. При решении задачи выбора рациональной архитектуры ПОФУ для разрабатываемой или модернизируемой НИС целесообразно использовать процедуры, построенные на основе многошаговых методов принятия решений [5], требующих от лица, принимающего решение (ЛПР), малого объема информации, заключающегося только в определении на каждом шаге только номера критерия, который по мнению ЛПР целесообразно улучшить.

При этом наиболее важным остается вопрос о свертке вектора критериев в скалярную целевую функцию. Поскольку все элементы множества $\mathbf{P}(H^{st})$ перспективных (Парето-оптимальных) вариантов архитектур ПОФУ НИС несравнимы (не имеют преимуществ друг перед другом), то любой элемент теоретически может быть наилучшим в соответствии с некоторым предпочтением ЛПР. Другими словами, вид скалярной целевой функции $Q\left(\alpha, W\left(h_i^{st}\right)\right)$ должен быть такой, что для любого $h_*^{st} \in P\left(H^{st}\right)$ должен существовать вектор α_r из множества возможных векторов M_α, обеспечивающий экстремум $Q\left(\alpha, W\left(h_i^{st}\right)\right)$, то есть

$$\forall h_*^{st} \in P\left(H^{st}\right) \exists \alpha_r \mid h_*^{st} = \arg\operatorname*{ext}_{h_i^{st}} Q(\alpha_r, W), h_*^{st} \in P\left(H^{st}\right), \alpha_r \in M_\alpha. \quad (1)$$

Наиболее часто употребляется линейная свертка критериев, базирующаяся на теореме С. Карлина. Согласно этой теореме, если множество допустимых альтернативных решений H^{st} выпукло, а все компоненты вектора цели W длины N вогнуты, то для любого решения h_*^{st}, принадлежащего множеству эффективных решений $h_*^{st} \in P\left(H^{st}\right)$ существует неотрицательный вектор α^* коэффициентов предпочтения длины N.

$\alpha^* = \{\alpha_i\}, \alpha_i \geq 0, \sum_{i=1}^{N} \alpha_i = 1,$ такой, что линейная свертка $\sum_{i=1}^{N} \alpha_i W_i\left(h_j^{st}\right)$ достигает своего экстремума в точке h_*^{st} на множестве H^{st}. Альтернативой является использование в качестве целевой функции логической (минимаксной) свертки Ю.Б. Гермейера [6]. В этом случае требование выпуклости множества допустимых альтернатив не предъявляется. Согласно теореме Гермейера, если решение h_*^{st} принадлежит множеству эффективных решений $h_*^{st} \in P\left(H^{st}\right)$, то существует неотрицательный вектор коэффициентов предпочтения α^* длины N $\alpha^* = \{\alpha_i\}, \alpha_i \geq 0, \sum_{i=1}^{N} \alpha_i = 1,$ такой, что логическая свертка $\min_i \alpha_i W_i\left(h_*^{st}\right)$ достигает своего максимума в точке h_*^{st} на множестве $P\left(H^{st}\right)$.

Человеко-машинная процедура поиска наиболее предпочтительного варианта сводится к следующему.

На фазе оптимизации первого шага в зависимости от наличия информации определяется начальный вектор предпочтений $\alpha^{(0)}$ и на его основе определяется наилучшее для данного шага решение $\breve{h}_*^{st}$.

На фазе анализа ЛПР оценивает полученную информацию и принимает решение о необходимости улучшения того или иного критерия $I_{ЛПР}$:

$I_{ЛПР} = 0$, если ЛПР удовлетворено полученным решением;

$I_{ЛПР} = i$, если ЛПР считает необходимым улучшить i-й показатель качества.

Фазы оптимизации последующих шагов отличаются от фазы оптимизации первого шага в части формирования вектора предпочтений $\alpha^{(i)}$. На фазе оптимизации i-го шага оценивается запас устойчивости вектора предпочтений $\varepsilon\left(\alpha^{(i-1)}\right)$ по решению $\breve{h}_{*(i-1)}^{st}$, полученного на $(i-1)$ шаге. По запасу устойчивости вектора предпочтений $\varepsilon\left(\alpha^{(i-1)}\right)$ определяется величина изменения μ компонент вектора предпочтений и определяется новый вектор предпочтений $\alpha^{(i)}$.

Поскольку очередной вектор коэффициентов предпочтения формируется путем изменения нужного компонента на фиксированную конечную величину μ на интервале]0..1[, то множество всех возможных векторов коэффициентов предпочтения M_α конечно и дискретно. В соответствии с (1) задача многошаговой оптимизации решается корректно, если отображение

$$\zeta : M_\alpha \to P\left(H^{st}\right) \tag{2}$$

является сюръекцией, то есть каждый элемент множества $P\left(H^{st}\right)$ является образом хотя бы одного элемента из множества M_α.

Проведенные исследования для линейной и нелинейной сверток векторного критерия W показали, что при нелинейной целевой функции $Q_{нл}$ отображение (2) является сюръекцией только при достаточно малой величине изменения μ. Что касается линейной целевой функции $Q_л$, то при изменении величины μ состав выбранных эффективных решений не меняется (в отдельных случаях может меняется незначительно), сюръекции отображения (2) не обеспечивается при сколь угодно малой μ. Это обстоятельство позволяет сделать вывод о том, что применение линейной свертки в качестве целевой функции некорректно для решения задачи выбора архитектуры ПОФУ вследствие не выпуклости дискретного множества H^{st}.

Кроме этого, количество векторов $\boldsymbol{a}$ множества M_α, являющихся прообразами того или иного решения h_i^{st} из $P\left(H^{st}\right)$ пропорционально расстоянию от этого решения до других, ближайших решений в пространстве параметров H^{st}.

Однако, вместе с тем, при количестве критериев больше двух появляются локальные, несвязанные между собой, зоны одного решения в пространстве векторов M_α. Это означает, что для одного и того же решения запас устойчивости может быть разным в зависимости от местонахождения начального решения в пространстве векторов $\boldsymbol{\alpha}$.

Другими словами, при выполнении многошаговой процедуры двигаясь в определенном направлении (увеличивая определенный компонент вектора $\boldsymbol{\alpha}$) можно перейти от одного решения к другому, а потом вновь вернуться к предыдущему решению не меняя направление поиска. Такая ситуация возникает не везде в пространстве M_α. Результаты моделирования показывают, что такие локальные зоны распределены не равномерно, а группируются ближе к началу координат и концам осей, то есть там, где один из компонентов вектора $\boldsymbol{\alpha}$ (а, следовательно, и соответствующий компонент векторного критерия W) является явно доминирующим**.** Так, например, в трехмерном пространстве M_α (трехкомпонентный критерий W) такие локальные зоны возникают только тогда, когда значение одного из компонент вектора $\boldsymbol{\alpha}$ превысит 0,6, то есть на него приходится более 60% общего веса коэффициентов.

Следовательно, если многошаговая процедура была остановлена ЛПР в тот момент, когда текущий вектор коэффициентов предпочтения имеет явно доминирующую составляющую, требуется дополнительное исследование устойчивости полученного решения.

Заключение

1. Процедура решения задачи синтеза архитектуры подсистемы обеспечения функциональной устойчивости навигационно-информационной системы включает два этапа. На первом этапе формируется множество эффективных вариантов архитектур ПОФУ путем Парето-оптимизации по векторному критерию эффективности, на втором– выбор рациональной архитектуры из множества эффективных вариантов на основе обобщенного критерия, учитывающего предпочтения лица, принимающего решения, с использованием человеко-машинных методов многокритериальной оптимизации.

2. Использование линейной свертки векторного критерия для выбора рационального варианта ПОФУ является некорректным вследствие дискретности множества вариантов архитектуры ПОФУ. Для его применения необходимо проводить серьезные исследования этого множества на выпуклость. Бес такого исследования целесообразно применение обобщенного критерия на основе логической свертки Ю. Гермейера.

3. При использовании человеко-машинных процедур многокритериальной оптимизации в случае наличия доминирования какого-либо компонента вектора предпочтений ЛПР необходимо проводить дополнительные исследования в окрестности полученного решения с целью определения его устойчивости.

Список литературы

1. Королев, А. Н. О функциональной устойчивости навигационно-информационных систем / А. Н. Королев, А. А. Тарасов // Вестник РГГУ. – 2012. – № 14/12. – С. 144–152.

2. Вязгин, В. А. Математические методы автоматизированного проектирования / В. А. Вязгин, В. В. Федоров. – М. : Высш. шк., 1989.

3. Айзерман, М. А. Выбор вариантов: основы теории / М. А. Айзерман, Ф. Т. Алескеров. – М. : Наука, 1990.

4. Данчул, А. Н. Системотехнические задачи создания САПР / А. Н. Данчул, Л. Я. Полуян ; под ред. А. В. Петрова. – М. : Высшая шк.,1990. – 144 с.

5. Степанов, А. В. Человеко-машинная процедура принятия решений в задачах векторной оптимизации / А. В. Степанов // Математическое моделирование. – 1991. – Т. 3, № 5. – С. 61–73.

6. Гермейер, Ю. Б. Введение в теорию исследования операций / Ю. Б. Гермейер. – М. : Наука, 1971.

УДК 519.81

МОДЕЛЬ РЕАЛИЗАЦИИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИХ ВОЗДЕЙСТВИЙ НА БОЛЬШИЕ СОЦИАЛЬНЫЕ ГРУППЫ

С.П. ЛАРИН, Е.А. РАФАЛЬСКАЯ
Государственное учреждение «Научно-исследовательский институт Вооруженных Сил Республики Беларусь», г. Минск, Республика Беларусь

В общем виде процесс оказания информационно-психологических воздействий (ИпВ) на большие социальные группы (БСГ) идентичен системе управления сложными организационными системами, основными элементами которых являются субъект(ы) и объект(ы) управления, а также связи между ними. При этом используется значительное количество каналов для оказания таких воздействий, что вызывает сложности в анализе информационного потока и принятии решений относительно проведения организационных или информационных мероприятий, направленных на снижение (нейтрализацию) негативных информационных воздействий на БСГ. Следует отметить, что в большинстве случаев для принятия таких решений не требуется точный прогноз. Важнее оперативно выявить факт ИпВ, его тематическую направленность и целевую аудиторию с точки зрения определения (прогнозирования) ее поведенческой реакции.

На основании изложенного, информационный поток целесообразно анализировать на предмет выявления тех сообщений, вызывающих негативные эмоциональные состояния (НЭС) БСГ. Следовательно, разработка модели реализации ИпВ на БСГ является важной и актуальной задачей.

Анализ проведенных исследований специалистов в области психологии, в первую очередь социальной [1, 2], показал наличие взаимосвязи поведения БСГ с такой категорией, как базовые ценности, что позволяет использовать их в модели в качестве основной характеристики БСГ.

На основе анализа статистических данных [2] были выделены типовые БСГ Республики Беларусь, проанализированы характерные для них базовые ценности, а также дана им количественная оценка, представленная в таблице 1.

Таблица 1

Количественные значения базовых ценностей для БСГ Республики Беларусь

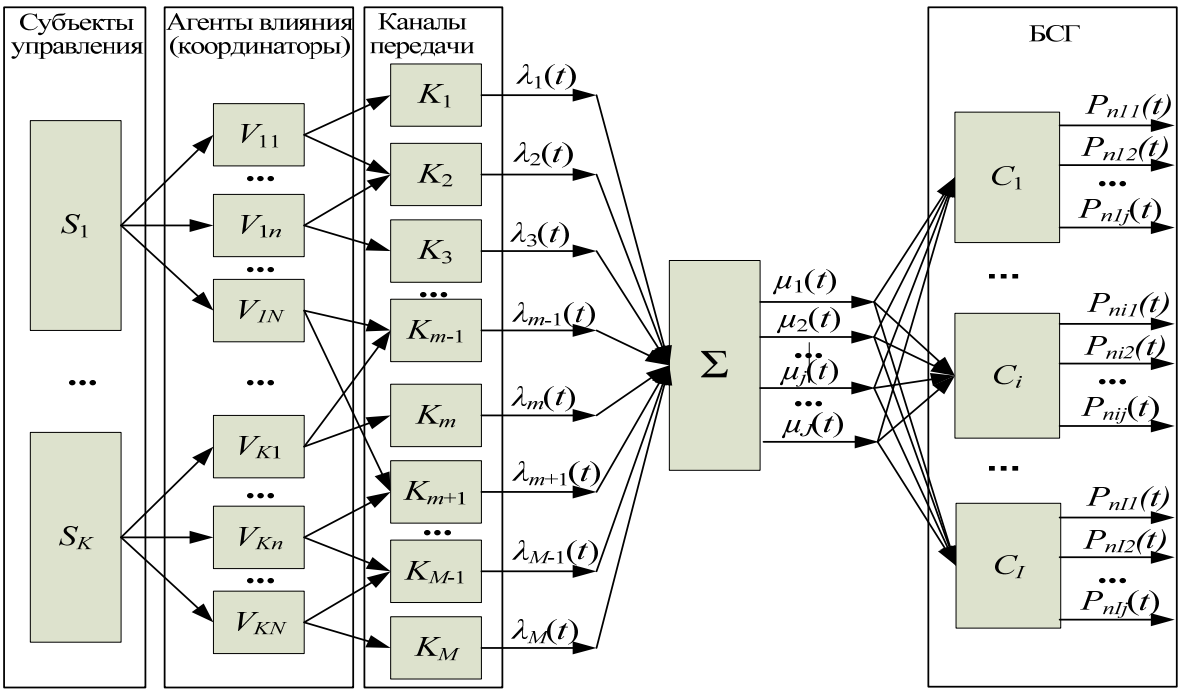
Базовые ценности	БСГ		
	Молодежь, %	Трудоспособное население, %	Пенсионеры, %
Жизнь и здоровье	67,50	68,60	70,70
Порядок (безопасность)	53,60	54,20	57,80
Общительность	45,50	41,00	49,80
Семья	46,00	49,50	54,80
Свобода	46,00	42,60	40,60
Благополучие	44,00	44,30	48,90
Независимость	39,70	37,20	35,50
Работа	33,30	28,60	25,40
Инициативность	28,80	19,70	19,40
Нравственность	27,50	26,10	30,10
Традиция	21,80	22,90	33,30
Жертвенность	19,50	21,10	28,60
Своевольность	10,60	8,00	6,60
Властность	8,70	6,20	5,70

Как следует из таблицы, ценностным фундаментом белорусского общества выступает неприкосновенность человеческой жизни, значимость личной безопасности, гарантом которой является закон, важность института семьи и достижение благополучия. Исходя из вышеизложенного, информационный поток целесообразно анализировать на предмет выявления контента, актуализирующий негативный (позитивный) образ относительно каждой из выделенных базо-

вых ценностей, с учетом их значимости для представителя БСГ. На основе выделенных ценностей, разработана модель реализации ИпВ на БСГ, представленная на рисунке 1. В интересах верификации модели тремя экспертами проведен анализ информационного контента сайта TUT.by с июля по сентябрь 2020 года. Было обработано более 4 тыс. информационных сообщений и определены количественные значения интенсивностей $\lambda_n(t)$ и $\lambda_p(t)$ для каждой базовой ценности. Результаты проведенного анализа представлены на рисунке 2 [3].

Как видно на рисунке 2, информационный контент до значимого социального события (выборы) по вышеуказанным базовым ценностям характеризуется всплесками, что подтверждает наличие целенаправленного информационного воздействия на БСГ именно в контексте менталитета белорусского общества.

Результаты проведенного сентимент-анализа показали, что значительное количество сообщений имели отрицательную модальность, особенно в отношении таких базовых ценностей, как жизнь (здоровье), право (безопасность), свобода. Данное обстоятельство явилось предпосылкой и инициацией массовых протестов, посвященных вышеуказанному важному политическому событию. Исходя из изложенного следует, что целенаправленное и планомерное воздействие посредством средств массовой информации (СМИ) на базовые ценности белорусского общества может привести к негативным эмоциональным состояниям БСГ и соответствующим поведенческим реакциям. Данную зависимость и отражают полученные результаты.



S_k, $k = 1, K$ – субъекты ИпВ;

V_{kn}, $n = 1, N$ – агенты влияния (координаторы) k-го субъекта ИпВ;

K_m, $m = 1, M$ – каналы передачи ИпВ;

$\lambda_m(t)$ – интенсивность информационного воздействия, количество сообщений в сутки от *m-го* канала передачи ИпВ;

C_i, $i = 1, I$ – БСГ;

$\mu_j(t)$, $j = 1, J$ – интенсивность информационного воздействия j-ую базовую ценность БСГ

$P_{nij}(t)$ – вероятность формирования негативного образа относительно j-ой базовой ценности у i-ой БСГ

Рис. 1. Модель реализации ИпВ на БСГ

Таким образом, для анализа информационного потока, циркулирующего в информационных сетях (СМИ, социальные сети и т. д.) разработана модель оказания ИпВ на БСГ. Особенностью данной модели является учет базовых ценностей белорусского общества как основной характеристики БСГ. Исследование в рамках данной модели позволит выявить специфи-

ку изменения НЭС БСГ в зависимости от потока информационных сообщений различной тематической направленности и модальности. Это позволит выявлять факты оказания ИпВ на население республики, анализировать информационный контент с учетом особенностей данного влияния на выделенные БСГ, исследовать применяемые противостоящей стороной способы манипулирования общественным мнением, формирования и провоцирования НЭС, добиться своевременного принятия мер по нейтрализации или недопущению указанных воздействий.

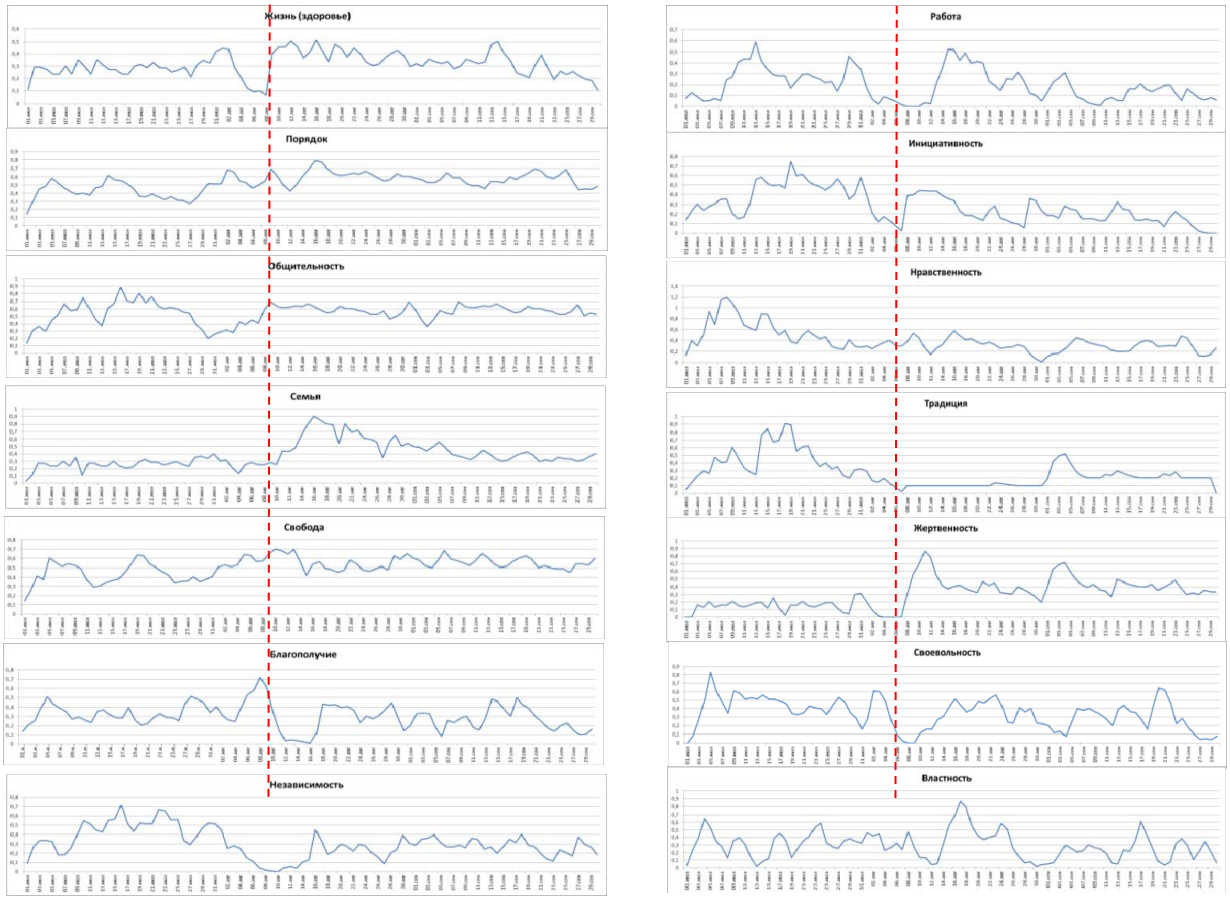


Рис. 2. Вероятностная оценка формирования негативных образов относительно выделенных базовых ценностей

Модель позволяет выявить специфику изменения НЭС БСГ в зависимости от потока информационных сообщений различной тематической направленности. Это позволит определить факты оказания ИпВ на население республики, анализировать информационный контент с учетом особенностей данного влияния на выделенные БСГ, исследовать применяемые противостоящей стороной способы манипулирования общественным мнением, формирования и провоцирования НЭС, добиться своевременного принятия мер по нейтрализации или недопущению указанных воздействий.

Список литературы

1. Лапин, Н. И. Структура ценностей россиян: всероссийский мониторинг и портрет региона // Опыт подготовки социокультурных портретов регионов России : материалы III-й всерос. науч.-практ. конф. – Курск : изд-во Курс. гос. университета, 2007. – С. 43–55.

2. Лашук, И. В. Социокультурный анализ современного белорусского общества / И. В. Лашук // Ин-т социологии Нац. акад. наук Беларуси. – Минск : Бел. навука, 2019. – 267 с.

3. Прогнозирование поведения информационно-психологических объектов при изменении их эмоциональных состояний : отчет о НИР, шифр «Вереск-И» // ГУ «НИИ ВС РБ» ; рук. С. П. Ларин – Минск, 2020. – 130 с.

УДК 621.391.8

УСТРОЙСТВО ДЕКОДИРОВАНИЯ РЕВЕРСИВНЫХ КОДОВ БОУЗА-ЧОУДХУРИ-ХОКВИНГЕМА С ДОПОЛНИТЕЛЬНЫМИ КОРРЕКТИРУЮЩИМИ ВОЗМОЖНОСТЯМИ ДЛЯ КОНТРОЛЯ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ

Г.А. ВЛАСОВА

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

При передаче, обработке и распределении, а также при хранении в запоминающих устройствах, возможно искажение информации из-за помех либо отказа ячеек памяти. Эффективным методом обнаружения, идентификации и коррекции ошибок является помехоустойчивое кодирование. При передаче сообщения в пространстве или во времени, то есть при хранении информации, помеха может иметь длительность большую, чем длительность одного символа передаваемого сообщения. В этом случае возникают пакетные ошибки – совокупность символов, которые начинаются и заканчиваются ошибочными символами, либо модульные ошибки, когда ошибочные символы сосредоточены в заданных границах (обычно длина модуля кратна байту).

Одними из лучших кодов, корректирующих независимые ошибки, являются коды Боуза-Чоудхури-Хоквингема (БЧХ). Реверсивный БЧХ-код, корректирующих две независимые ошибки, задается проверочной матрицей $H = (H_1, H_2)^T = (\alpha^i, \alpha^{-i})^T$, где α-примитивный элемент поля Галуа $GF(2^m)$, $m \geq 3$; $0 \leq i \leq n-1$, $n = (2^m - 1)$ – длина кодовой последовательности [1].

Пусть $H_m = (h_{1m}, h_{2m}, I)^T$ – проверочная матрица $(2^m,\ 2^m - 2m - 1)$ – кода, полученная из матрицы H реверсивного БЧХ-кода перестановкой столбцов (то есть разрядов кодового слова) по правилу $\alpha^i \to i$ ($i = [1,\ 2,\ \ldots, 2^m - 1]$, нулевой столбец остается на месте). В этом случае столбцы подматрицы h_{1m} (элементы поля $GF(2^m)$) представляют собой m-разрядные двоичные числа $0,\ 1,\ 2, \ldots, 2^m - 1$, расположенные в лексикографическом порядке. Подматрица I – строка, состоящая из единиц. Столбцы проверочной матрицы H_m последовательно разделяются на 2^{m-2} модуля длины четыре. В [2, 3] показано, что модифицированный реверсивный БЧХ-код, задаваемый матрицей H_m, корректирует не только двойные независимые ошибки (как классический БЧХ-код с расстоянием $d = 5$), но и одиночные модули ошибок длины четыре, а также пакетные ошибки длины три. При этом необходимо, чтобы след элемента $\beta = (1 + \alpha + \alpha^2)^{-1}$ был равен единице $(Tr(\beta) = 1)$.

Аппаратные и временные затраты, необходимые для обработки кода определяются устройством декодирования.

Алгоритм декодирования модифицированного $(2^m,\ 2^m - 2m - 1)$- кода БЧХ с проверочной матрицей H_m [2]:

1. Вычисляется синдром $S = (S_1, S_2, S_3)^T$ – декодируемого слова X:

$S = X \cdot H_m^T,\ S_1 = X \cdot h_{1m}^T,\ S_2 = X \cdot h_{2m}^T,\ S_3 = X \cdot I^T$;

2. По виду синдрома определяется вид ошибки E (при нулевом синдроме $(S_1 = S_2 = S_3 = 0)$ считается, что ошибок нет);

3. Полученный вектор ошибки E суммируется по модулю два с декодируемым словом X, то есть ошибки корректируются.

Первый и последний пункты алгоритма декодирования реализуются сумматорами по модулю два и их вклад в аппаратные затраты на декодирование не значителен. Сначала для вычисления каждого *j*-го символа синдрома S суммируются по модулю два разряды декодируемого слова X, которым соответствуют единичные символы в *j*-ой строке проверочной матрицы H_m (*j* принимает значения от 1 до $2m+1$). На заключительном этапе обработки используют 2^m двухвходовых сумматоров по модулю два.

Основной проблемой при обработке кодов является построение селектора (пункт 2 алгоритма), то есть устройства, по виду синдрома определяющему вид ошибки (номера ошибочных разрядов в декодируемой последовательности). Очевидным (и при этом самым быстрым) решением является использование запоминающего устройства (ЗУ), в котором по адресу синдрома хранится вектор ошибок. Количество хранимых 2^m- разрядных векторов ошибок равно сумме всех возможных независимых (одиночных и двойных), а также модульных и пакетных ошибок и составляет

$$K_{\text{нез}} + K_{\text{мод}} + K_{\text{пакет}} = \sum_{i=1}^{t} C_n^{\,i} + (2^m + 2^{m-2}) + 2^{m-1} = \sum_{i=1}^{t} C_n^{\,i} + 7\cdot 2^{m-1},\ t = 2.$$

Количество модулей равно 2^{m-2}, а все возможные модульные ошибки длины четыре имеют вид (1110), (0111), (1011), (1101), (1111). Поэтому число всех модульных ошибок на длине декодируемого слова равно $5\cdot 2^{m-2} = (2^m + 2^{m-2})$. Количество пакетных ошибок длины три составляет $2\cdot 2^{m-2} = 2^{m-1}$, поскольку необходимо рассмотреть лишь ошибки веса три на границах модулей: (1|11) и (11|1).

С увеличением длины кодового слова скорость кода, определяемая как отношение числа информационных разрядов к длине декодируемого слова, то есть к сумме информационных и дополнительных проверочных разрядов, возрастает. Поэтому при проектировании устройств обработки стремятся использовать коды большой длины. Однако, как показано выше, количество селектируемых комбинаций, необходимых для коррекции ошибок, при этом резко возрастает.

Сократить в $2^m - 1$ раз количество хранимых векторов одиночных и двойных ошибок позволяет разделение ошибок на классы [3]. Каждый класс ошибок состоит из $(2^m - 2)$ циклического сдвига образующего. Класс характеризуется весом ошибки, расстоянием между ошибочными разрядами и параметрами идентификации N_u. Для реверсивного БЧХ-кода, корректирующего две независимые ошибки и задаваемого проверочной матрицей H, параметр идентификации класса ошибок определяется как $N = (p+q) \bmod (2^m - 1)$, причем $S_1 = X \cdot {H_1}^T = \alpha^p$, $S_2 = X \cdot {H_2}^T = \alpha^q$. Вычислив значение синдрома и параметра N, можно определить класс, к которому относится ошибка, а, следовательно, и образующий класса с синдромом $S = (\alpha^{p0}, \alpha^{q0})$. Фактический вектор ошибок определяется по сдвигу $(p - p0) \bmod (2^m - 1)$. Чтобы применить метод разделения независимых ошибок на классы к модифицированным реверсивным БЧХ-кодам, задаваемым матрицей H_m, достаточно реализовать перестановку разрядов в соответствии с порядком следования столбцов в матрице H. Следует отметить, что перестановка разрядов в кодовом слове не влияет на сложность устройства.

Таким образом, разделение ошибок на классы подмножеств позволяет практически в $n = (2^m - 1)$ раз уменьшить сложность селектора. Вносимые при этом дополнительные временные затраты не значительны и определяются временем дешифрации (определения значений p и q по значениям α^p и α^q), вычислением параметра идентификации класса ошибок $N = (p+q) \bmod (2^m - 1)$ и вычислением значения сдвига $(p - p0) \bmod (2^m - 1)$ фактического вектора ошибок относительно образующего класса. Применение устройств обработки моди-

фицированных БЧХ-кодов позволяет обеспечить целостность (неизменность) информации в условиях воздействия не только независимых одиночных и двойных ошибок, но и модульных ошибок длины четыре, а также пакетных ошибок длины три.

Список литературы

1. Мак-Вильямс, Ф. Дж. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. – М. : Связь, 1979. – 744 с.

2. Липницкий, В. А. Двоичные реверсивные коды для контроля байтовых ошибок / В. А. Липницкий [и др.] // Известия Нац. акад. наук Беларуси. Серия физико- математических наук. – 2000. – №1. – С. 127–131.

3. Власова, Г. А. Разработка методов и устройств идентификации и коррекции ошибок кодами Боуза-Чоудхури-Хоквингема : автореф. дис. …канд. техн. наук: 05.12.21 / Г. А. Власова ; Бел. Гос .ун-т информатики и радиоэлектроники. – Минск, 1996. – 18 с.

УДК 004.056

ИСПОЛЬЗОВАНИЕ TLA+ ДЛЯ ОПИСАНИЯ МОДЕЛИ ИЗОЛИРОВАННОЙ ПРОГРАММНОЙ СРЕДЫ СУБЪЕКТОВ ДОСТУПА

А.М. КАННЕР
Закрытое акционерное общество «ОКБ САПР», г. Москва, Российская Федерация

В работах [1, 2] описана необходимость в проведении моделирования и верификации средств защиты информации (СЗИ), а также перечислены конкретные нормативные документы Российской Федерации, в которых предъявляются требования в части верификации их функций защиты. Современные инструментальные средства верификации позволяют в автоматическом режиме проверить выполнение некоторых формальных свойств при работе СЗИ. Однако еще более примечательным преимуществом средств верификации является возможность в автоматическом режиме проверять математические модели безопасности компьютерных систем.

Большинство известных формальных моделей безопасности (Белла-ЛаПадула, Харрисона-Руззо-Ульмана и др.) сформулированы в математической нотации, с использованием подходящего для этого математического аппарата. При этом основным компонентом любой формальной модели является базовая теорема безопасности, с помощью которой обосновываются некоторые формальные свойства, гарантирующие безопасность системы или обрабатываемых в ней данных.

Однако любая формальная модель в математической нотации имеет достаточно сложное описание, а ошибки в базовой теореме безопасности или в самой нотации может выявить только квалифицированный специалист-математик. Кроме того при проверке математической нотации нельзя исключать человеческий фактор – в результате в модели могут существовать скрытые недостатки, которые крайне сложно выявить и исправить. Так как модели безопасности часто используются как фундамент для теоретической гарантии некоторых свойств безопасности в компьютерных системах, критически важной задачей становится проверка этих моделей на наличие ошибок.

В задаче проверки формальных моделей безопасности могут помочь средства верификации. Для этого математическую нотацию необходимо перевести в нотацию на некотором формальном языке, пригодном для верификации (TLA+, EventB и др.), а затем сформулировать условия базовой теоремы безопасности в виде инвариантов или темпоральных свойств. В результате это позволяет:

1. Исключить человеческий фактор при проверке модели безопасности.
2. Проводить верификацию силами менее квалифицированных специалистов (с помощью запуска средств верификации).
3. Проверять выполнение условий базовой теоремы безопасности во всевозможных состояниях моделируемой системы.
4. Выявлять скрытые ошибки в математической нотации.

В [3] автором описана первая версия математической нотации модели изолированной программной среды субъектов доступа (ИПСС), которая является развитием субъектно-ориентированной модели изолированной программной среды (ИПС) [4, 5]. В отличие от ИПС в модели ИПСС производится другая декомпозиция системы на сущности: субъектами являются пользователи и системные сервисы (а не процессы пользователей, как в ИПС), а объектами – функционально ассоциированные с этими субъектами объекты (процессы) и объекты-данные с возможностью динамического изменения их состава во времени. Отличительной особенностью модели ИПСС является учет подсистемы защиты в качестве сущности системы, такой же, как и другие субъекты системы, и обоснование невозможности нарушения действующих правил управления доступом за счет свойства абсолютной корректности (изолированности) субъектов доступа.

К сожалению, математическая нотация модели не позволяет гарантировать выполнения формальных свойств безопасности во всех возможных состояниях системы, а экспериментальные исследования реализаций этой модели на практике требуют повторного про-

ведения даже при малых усовершенствованиях модели. В связи с этим в [6] проведена верификация модели ИПСС с использованием темпоральной логики действий Лэмпорта (TLA+) и метода *Model Checking*.

Спецификация модели ИПСС в TLA+ имеет следующие компоненты:

1. Начальное состояние – инициализация системы (Init), пример предиката инициализации модели ИПСС приведен на рисунке 1.

2. Переменные модели – сущности, которые могут изменяться в процессе работы (субъекты, объекты и др.).

3. Правила работы системы – возможные состояния и значения переменных модели, правила перехода из состояния в состояние – например, при осуществлении доступов субъектов к объектам.

4. Теорема, доказываемая при верификации и проверяющая специальные предикаты (формальные свойства системы) – инварианты и темпоральные свойства.

```
Init
Инициализация модели
Init ≜  ∧ S_active = {s_0}
          изначально существует только s_0 и его процесс o_0
        ∧ O_func = {o_0}
        ∧ O_data = {}
        ∧ O_na = {o_sorm, o_2}
          остальные субъекты еще не активизированы
        ∧ S = {s_0, s_sorm, s_2, s_3, s_4}
        ∧ Q = ⟨q_0⟩
```

Рис. 1. Начальное состояние системы, описывающее переменные – активные и неактивные субъекты доступа, доступные объекты доступа, последовательность доступов

В качестве действий в системе могут совершаться запросы модели ИПСС: создание и удаление процессов, создание пользователей и системных субъектов, удаление субъектов, а также чтение, запись, создание, удаление и исполнение объектов доступа. Предусловиями являются предикаты, выполнение которых необходимо для совершения действия. Постусловия определяют каким образом после выполнения действия изменяются переменные модели, то есть какое новое состояние будет иметь система. Пример одного из действий системы, описанного в виде предикатов пред- и пост-условий его выполнения приведен на рисунке 2.

```
ReadD
Реализация информационного потока на чтение
Read(s, o, o_r) ≜
        Процесс читает данные и изменяет свое состояние
        ∧ IF o_r.state ≠ s_0.sid
          THEN O_func' = (O_func \ {o}) ∪
                         {[o EXCEPT !["state"] =
                           o_r.state]}
          ELSE O_func' = O_func
        Объект с данными становится ассоциированным
        ∧ O_data' = (O_data \ {o_r}) ∪
          {[oid ↦ o_r.oid,
            type ↦ "data",
            subj_assoc ↦ (o_r.subj_assoc ∪ {s.sid}),
            state ↦ o_r.state]}
        ∧ O_na' = O_na \ {o_r}
        ∧ Q' = Append(Q, [subj ↦ s,
                          proc ↦ (CHOOSE f ∈ O_func' : f.oid = o.oid),
                          dent ↦ (CHOOSE d ∈ O_data' : d.oid = o_r.oid),
                          type ↦ "read"])
        ∧ UNCHANGED ⟨S_active, S⟩

ReadD ≜
        ∃ s ∈ S_active :
        ∃ o ∈ SelectSubjProc(s) :
        ∃ o_r ∈ SelectObjects \ SelectProc :

          Правила доступа s_sorm
          ∧ SormCheckPerm(s, o_r, "read")

          Постусловия
          ∧ Read(s, o, o_r)
```

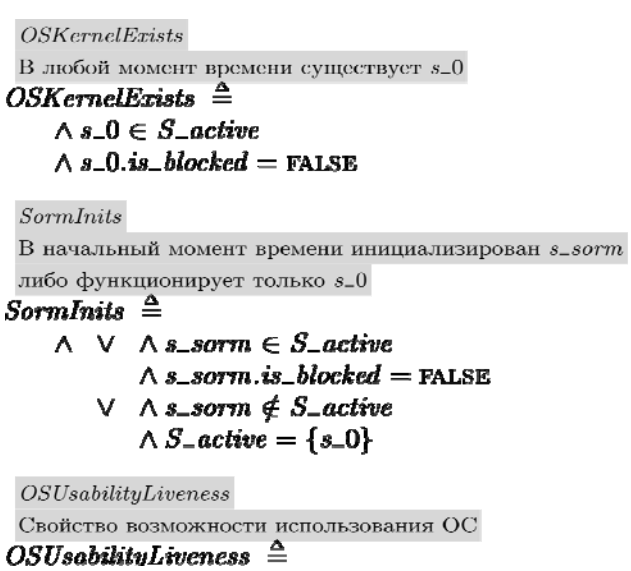
Рис. 2. Пост- и пред-условия для запроса на чтение объекта доступа

При доказательстве теоремы в ходе верификации проверяется истинность специальных предикатов – инвариантов или темпоральных свойств, приведенных на рисунке 3. Инварианты должны выполняться во всех состояниях и для каждой реализации системы, а также за счет использования последовательности совершенных запросов к системе могут проверять условия, произошедшие в прошлом, например, при последнем переходе системы. Темпоральные свойства, в отличие от инвариантов, могут применять специальные темпоральные операторы TLA+ [6, 7], с помощью которых можно составлять предикаты, зависящие от времени выполнения и определенных событий в прошлом или будущем.


Invariants and Temporal Properties
Теорема, учитывающая инварианты и свойства: доказывается при верификации
THEOREM $Spec \Rightarrow \land \Box TypeInv$
$\land \Box ConsistencyInv$
$\land \Box BlockedInv$
$\land \Box OSKernelExists$
$\land \Box SormInits$
$\land \Box Correctness$
$\land \Box AbsCorrectnessOpp$
$\land OSUsabilityLiveness$
$\land AbsCorrectness$

Рис. 3. Теорема, проверяемая при верификации спецификации модели ИПСС

В ходе создания TLA+ нотации модели ИПСС были выявлены скрытые ошибки, допущенные в математической нотации. Так, например, нарушались инварианты свойств корректности модели ИПСС, и один субъект мог опосредованно воздействовать на другой субъект доступа через операции порождения. Также была выявлена возможность некорректной работы самой моделируемой системы – она проходила этап инициализации, и далее в реализации было еще несколько состояний, но на определенном состоянии система переставала работать еще до появления пользователей, так как завершал работу единственный системный процесс (ядро ОС). Аналогично была выявлена ошибка с возможностью работы системы при завершении работы субъекта, разграничивающего доступ (подсистемы управления доступом), или при удалении объекта, содержащего применяемые правила доступа.


OSKernelExists
В любой момент времени существует s_0
$OSKernelExists \triangleq$
$\land s\_0 \in S\_active$
$\land s\_0.is\_blocked = \text{FALSE}$

SormInits
В начальный момент времени инициализирован s_sorm либо функционирует только s_0
$SormInits \triangleq$
$\land \lor \land s\_sorm \in S\_active$
$\land s\_sorm.is\_blocked = \text{FALSE}$
$\lor \land s\_sorm \notin S\_active$
$\land S\_active = \{s\_0\}$

OSUsabilityLiveness
Свойство возможности использования ОС
$OSUsabilityLiveness \triangleq$

Рис. 4. Дополнительные инварианты для устранения недостатков математической нотации модели ИПСС

Таким образом, при исправлении выявленных ошибок в TLA+ нотации кроме модификации свойств корректности и некоторых операций модели ИПСС были добавлены инварианты, представленные на рисунке 4:

1. *OSKernelExists* – инвариант для контроля работоспособности системы (постоянное наличие системного субъекта – ядра ОС).
2. *SormInits* – инвариант для контроля активизации подсистемы управления доступом.
3. *OSUsabilityLiveness* – темпоральное свойство для проверки работоспособности системы: в любой реализации системы обязательно кроме начальных системных субъектов должен активизироваться пользователь или еще один системный субъект.

Полный текст разработанной спецификации модели ИПСС доступен на сайте автора https://github.com/kanner/ipes-model.

Проведенная верификация формальной модели ИПСС продемонстрировала то, что на сегодняшний день при разработке и проверке моделей безопасности компьютерных систем целесообразно в первую очередь использовать нотацию на формальных языках, пригодных для верификации. Классическая математическая нотация моделей безопасности имеет ряд существен-

ных недостатков, особенно в части верификации. В связи с этим ценность математической нотации постепенно теряется и на первый план выходит возможность автоматической проверки моделей безопасности во всех возможных состояниях системы с использованием инструментальных средств. Тем не менее, для удобства восприятия современные средства верификации позволяют транслировать описание модели с формального языка в математическую нотацию.

Использовать средства автоматической верификации также крайне удобно при написании новых моделей безопасности, так как логические ошибки можно устранять уже на раннем этапе, постепенно добавляя требуемые инварианты безопасности по мере описания основных операций модели.

Список литературы

1. Каннер, А. М. Подход к верификации подсистемы управления доступом операционной системы LINUX / А. М. Каннер // Комплексная защита информации: материалы XXV научно-практической конференции, 15–17 сентября 2020 г. – М. : Медиа Группа «Авангард», 2020. – С. 24–28.

2. Каннер, А. М. Моделирование и верификация подсистемы управления доступом средства защиты информации Аккорд-X / А. М. Каннер, Т. М. Каннер // Вопросы защиты информации. – 2020. – № 3. – С. 6–10.

3. Kanner, A. M. Correctness of Data Security Tools for Protection against Unauthorized Access and their Interaction in GNU/Linux / A. M. Kanner // Global Journal of Pure and Applied Mathematics. – 2016. – Vol. 12, № 3. – P. 2479–2501.

4. Щербаков, А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты / А. Ю. Щербаков. – М. : Книжный мир, 2009. – 352 с.

5. Щербаков, А. Ю. Хрестоматия специалиста по современной информационной безопасности / А. Ю. Щербаков. – Saarbrucken : Palmarium Academic Publishing, 2016. – 272 с.

6. Kanner, A. M. Verification of a Model of the Isolated Program Environment of Subjects Using the Lamport's Temporal Logic of Actions / A. M. Kanner, T. M. Kanner // Proceedings of the VII International Conference «Engineering & Telecommunication». – IEEE, 2021.

7. Kanner, A. M. Special Features of TLA+ Temporal Logic of Actions for Verifying Access Control Policies / A. M. Kanner, T. M. Kanner // Proceedings of Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology. – IEEE, 2021.

УДК 004.931

ЗАДАЧИ АВТОМАТИЧЕСКОЙ ОБРАБОТКИ ТЕКСТОВ НА ЕСТЕСТВЕННЫХ ЯЗЫКАХ В АСПЕКТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С.Ю. МЕЛЬНИКОВ
Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов», г. Москва, Российская Федерация

Введение. Стратегические направления научных исследований в области обеспечения информационной безопасности перечислены в «Доктрине информационной безопасности Российской Федерации», утвержденной Указом Президента РФ № 646 от 5 декабря 2016 г. [1] и в «Основных направлениях научных исследований в области обеспечения информационной безопасности Российской Федерации», утвержденными Секретарем Совета Безопасности Российской Федерации Н.П.Патрушевым 31 августа 2017 г. [2]. Во многом эти направления связаны с развитием автоматических методов обработки информации, для чего необходимо совершенствовать, в том числе, вычислительно-лингвистические методы автоматической обработки текстов.

1. Задачи ИБ, для решения которых необходима автоматическая обработка текстов. В настоящее время аппарат вычислительной лингвистики активно используется для решения ряда актуальных задач информационной безопасности. Перечислим некоторые из них:

– выявление скомпрометированных аккаунтов в социальных сетях [3],

– построение фильтров для анализа фишинговых атак [4],

– непрерывная идентификация пользователя по потоку его сообщений [5],

– обнаружение фейковых новостей [6], фейковых обзоров товаров и услуг [7],

– оценка достоверности систем учета мнений и анализа отзывов пользователей [8],

– обнаружение атак на веб-ресурсы, использующих автоматически сгенерированные тексты с незначительными изменениями контента [9],

– задачи выявления материалов деструктивной направленности [10],

– круг задач, связанных с обнаружением искусственно сгенерированных текстов [11],

– задачи, связанные с использованием избыточности языка в криптографических [12] и стеганографических [13] приложениях,

– задачи анализа искаженных текстов, в случае, когда искажения имеют случайное [14], умышленное [15] или неумышленное [16] происхождение,

– и ряд других задач.

2. Используемые методы вычислительной лингвистики. Перечисленные задачи используют методы вычислительной лингвистики, которые можно разделить на два типа.

Тип 1. Методы решения идентификационных задач, в которых проверяется гипотеза о том, что анализируемое сообщение (набор сообщений) принадлежит тому или иному классу из ограниченного множества. Результатом работы первого типа методов является прямое указание класса, либо вектор рандомизированных оценок принадлежности сообщения тому или иному классу.

Тип 2. Методы решения задач распознавания, в которых требуется построить определенную последовательность, связанную с анализируемым сообщением (потоком сообщений). Отличие второго типа методов состоит в том, что результатом их работы является последовательность классов либо векторов рандомизированных оценок, и длина этой последовательности растет с увеличением длины и числа анализируемых сообщений.

К первому типу относятся методы решения следующих задач:

– идентификация языка сообщения в предположении, что оно является моноязычным, а язык выбирается из заданного множества языков [17];

– идентификация авторства сообщения, в предположении, что оно написано одним автором, который принадлежит множеству известных. Авторы могут задаваться, например, своими авторскими коллекциями текстов [18];

– идентификация тематики, жанра, стиля, эмоциональной окраски сообщения, в аналогичных предположениях [19];

– определение происхождения (естественное/результат перевода/результат автоматического перевода/искусственное) текста анализируемого сообщения [20].

Ко второму типу относятся методы решения следующих задач:

– коррекция искаженного текста [21];

– разбиение текста на моноязычные фрагменты и идентификация языка каждого фрагмента [22];

– разбиение текста на фрагменты и идентификация авторства, тематики, жанра, стиля, эмоциональной окраски фрагментов в аналогичных предположениях [23];

– определение текстуальных заимствований в текстах [24];

– определение тех или иных связей между текстами [25].

Заключение. Проанализированы современные задачи автоматической обработки текстов, в интересах обеспечения информационной безопасности, для решения которых используются методы вычислительной лингвистики.

Список литературы

1. http://www.scrf.gov.ru/security/information/document5.
2. http://www.scrf.gov.ru/security/information/document155.
3. Barbon, S. Authorship verification applied to detection of compromised accounts on online social networks: A continuous approach / S. Barbon, R. Igawa, B. Zarpelão // Multimedia Tools and Applications. – 2017. – № 76 (3). – P. 3213–3233.
4. Duman, S. EmailProfiler: Spearphishing filtering with header and stylometric features of emails / S. Duman [et al.] // In Proceedings of the 2016 IEEE 40th Annual Computer Software and Applications Conference. – 2016. – Vol. 1. – P. 408–416.
5. Brocardo, M. Authorship verification using deep belief network systems / M. Brocardo [et al.] // International Journal of Communication Systems. – 2017. – № 30 (12). – P. 3259.
6. Третьяков, А. О. Метод определения русскоязычных фейковых новостей с использованием элементов искусственного интеллекта / А. О. Третьяков [и др.] // International Journal of Open Information Technologies. – 2018. – Vol. 6, № 12. – P. 99–105.
7. Layton, R. Identifying faked hotel reviews using authorship analysis / R. Layton, P. Watters, O. Ureche // In Proceedings – 4th Cybercrime and Trustworthy Computing Workshop, CTC ’13. – 2013. – P. 1–6.
8. Panicheva, P. Personal sense and idiolect: Combining authorship attribution and opinion analysis / P. Panicheva, J. Cardiff, P. Rosso // In Proceedings of the International Conference on Language Resources and Evaluation, LREC 2010.
9. Shahid, U. Accurate detection of automatically spun content via stylometric analysis / U. Shahid [et al.] // In Proceedings of the 2017 IEEE International Conference on Data Mining (ICDM). – 2017. – P. 425–434.
10. Iskhakova, A. Research of the estimated emotional components for the content analysis / A. Iskhakova, A. Iskhakov, R. Meshcheryakov // Journal of Physics: Conference Series. – 2019. – Vol. 1203. –P. 012065.
11. Исхакова, А. О. Метод определения искусственных текстов на основе расчета меры принадлежности к инвариантам / А. О. Исхакова // Труды СПИИРАН. – 2016. – № 6 (49). – С. 104-121.
12. Teahan, W. The Entropy Of English Using PPM-based Models, Proceedings of Data Compression Conference-DCC'96 / W. Teahan, J. Cleary. – IEEE Computer Society Press, 1996. – P. 53–62.
13. Alghamdi, N. Capacity Investigation of Markov Chain-Based Statistical Text Steganography: Arabic Language Case / N. Alghamdi, L. Berriche // In Proceedings of the 2019 Asia Pacific Information Technology Conference (APIT 2019). – ACM, New York, USA. – P. 37-43.
14. Германович, А. В. Информационные измерения языка. Программная система оценки читаемости искаженных текстов / А. В. Германович [и др.] // Известия ЮФУ. Технические науки. – 2019. – № 8. – С. 6–18.
15. Северин, Н. В. Методы нечеткого поиска в системах контроля нецелевого контента / Н. В. Северин // Вісник Східноукраїнського національного університету ім.В.Даля. – 2012. – № 8 (179), ч. 2. – С. 199–205.
16. Бирин, Д. А. Об эффективности средств коррекции искаженных текстов в зависимости от характера искажений / Д. А. Бирин [и др.] // Известия ЮФУ. Технические науки. – 2018. – № 8. – С. 104–114.
17. Кулай, А. Ю. О статистических методах идентификации языка, искаженных текстовых и речевых сообщений / А. Ю. Кулай, Д. А. Леднов, С. Ю. Мельников // Известия ЮФУ. Технические науки. – 2008. – № 8. – С. 177–183.
18. Iskhakova, A. The Approach to Minimize the Impostor Method Errors in the Author Identification Open Problem / A. Iskhakova [et al.] // Proceedings of the R. Piotrowski's Readings in Language Engineering and Applied Linguistics. S.Petersburg, Russia, November 27, 2019. CEUR Workshop Proceedings. – Vol. 2552. – P. 60–72.
19. Орлов, Ю. Н. Определение жанра и автора литературного произведения статистическими методами / Ю. Н. Орлов, К. П. Осминин // Прикладная информатика. – 2010. – № 2 (26). – С. 95–108.

20. Исхакова, А. О. Выбор параметров для идентификации искусственно созданных текстов / А. О. Исхакова // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2013. – № 2 (28). – С. 126-128.

21. Вахлаков, Д. В. Многоэтапный метод автоматической коррекции искаженных текстов / Д. В. Вахлаков, С. Ю. Мельников, В. А. Пересыпкин // Известия ЮФУ. Технические науки. – 2020. –№ 7. – С. 35-45.

22. Arjun, M. Y. Language Identification from a Tri-lingual Printed Document: A Simple Approach / M. Y. Arjun, H. G. Chirag // Int. Journal of Engineering Research and Applications. – 2014. – Vol. 4. – P. 132–136.

23. Elamine, M. An Unsupervised Method for Detecting Style Breaches in a Document / M. Elamine, S. Mechti, L. Belguith // 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA). – 2019. – P. 1–6.

24. Сафин, К. Ф. Определение заимствований в тексте без указания источника / К. Ф. Сафин, М. П. Кузнецов, М. В. Кузнецова // Информ. и ее примен. – 2017. – № 11(3). – С. 73–79.

25. Agirre, E. Semantic textual similarity / E. Agirre [et al.]// 2nd Joint Conference on Lexical and Computational Semantics. – 2013. – P. 32–43.

УДК 004.056.5

КРИТЕРИЙ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ПРИ ЕЕ УТЕЧКЕ ИЗ ВОЛС

В.А. ДМИТРИЕВ, Е.П. МАКСИМОВИЧ
Государственное научное учреждение «Объединенный институт проблем информатики Национальной академии наук Беларуси», г. Минск, Республика Беларусь

Передача информационных потоков по волоконно-оптическим линиям связи (далее – ВОЛС) имеет ряд преимуществ по сравнению с передачей данных посредством кабеля из медных материалов. К ним относится: высокая сопротивляемость электромагнитным помехам, широкая пропускная способность (вплоть до нескольких терабит в секунду), незначительное затухание сигнала, низкий уровень шума, повышенная защита информации.

В ВОЛС способ передачи информации основан на модуляции оптического излучения. Основные причины утечки информации в ВОЛС связаны с излучением световой энергии в окружающее пространство. Причины этого излучения обусловлены процессами, происходящими при вводе (выводе) излучения в ВОЛС и распространении волн в оптическом волокне. Кроме того, утечка информации за счет оптического излучения может иметь место из-за наличия постоянных и разъемных соединений оптических волокон, а также их изгибов и повреждений.

Одним из важнейших требований, предъявляемых к современным телекоммуникационным системам, является обеспечение скрытности и конфиденциальности связи. В волоконно-оптических линиях связи должна быть сформирована надежная, защищенная инфраструктура с использованием всех доступных средств и способов информационной защиты.

Одним из методов защиты информации от несанкционированного доступа при ее распространении в ВОЛС являются метод, основанный на использовании лазера, генерирующего импульсы оптического излучения столь малой длительности, что в пределах каждого импульса содержится один фотон, находящийся в состоянии линейной или круговой поляризации.

Поскольку оптическое волокно изготовлено из кварцевого стекла, то в качестве носителя информации необходимо использовать излучение полупроводникового лазера или лазерного диода в ближней инфракрасной области на длинах волн 850 мкм, 1300 мкм и 1550 мкм, которое являеся импульсным. На указанных длинах волн затухание оптического излучения в оптическом волокне является минимальным.

Критерием защищенности информации при ее утечке из ВОЛС является отношение сигнал/шум фотоэлектронов на выходе фотоприемника. Информация будет защищенной при ее утечке из ВОЛС, если будет выполняться следующее соотношение: $\delta \le \delta_0$, где δ_0 – предельно допустимое (пороговое) значение отношения сигнал/шум на входе в фотоприемник (отношение сигнал/шум фотоэлектронов). Целью работы является определение δ_0.

Самый простой и действенный способ защиты информации при ее утечке из ВОЛС – снижение мощности модулированного сигнала до безопасного уровня. Снижение мощности модулированного сигнала может обеспечить полную защищенность информации только от пассивного съема. При активном съеме полная защищенность информации не обеспечивается, но снижение мощности модулированного сигнала имеет большое значение, так как в этом случае нарушителю для перехвата потребуется выводить бóльшую мощность модулированного сигнала, что приведет к увеличению потерь в ВОЛС и упростит задачу обнаружения попытки съема. Для обнаружения слабого модулированного оптического излучения используется метод счета фотонов [1], который является одним из наиболее чувствительных методов регистрации слабого оптического излучения.

Поскольку излучение полупроводникового лазера и лазерного диода является импульсным и количество импульсов в неперекрывающихся временных интервалах статистически независимы, то согласно [2] статистика оптического излучения является пуассоновской.

Слабый оптический сигнал на выходе фотоприемника представляет собой последовательность флуктуирующих по амплитуде «одноэлектронных» импульсов [3]. Следует отметить, что статистика фотоэлектронов (фотоотсчетов), в плоскости чувствительного слоя фо-

топриемника повторяет статистику оптического излучения, падающего на фотоприемник, т. е. также является пуассоновской [4].

Тип шума аналогового фотоприемника, который преобразует демодулированное оптическое излучение, являющееся источником информации, которую необходимо защитить, в электрический сигнал (фотоэлектроны), зависит от частоты демодулированного оптического излучения. Если частота демодулированного оптического излучения $f \leq 100$ кГц, преобладающими шумами фотоприемника являются дробовые шумы с пуассоновской статистикой, а для частот демодулированного оптического сигнала $f > 100$ кГц, преобладающими шумами на фотоприемника являются тепловые шумы с гауссовской статистикой [5, 6].

Тип шума цифрового фотоприемника, который преобразует демодулированное оптическое излучение, являющееся источником информации, которую необходимо защитить, в электрический сигнал (фотоэлектроны), зависит от скорости передачи информации по ВОЛС. Когда скорость передачи информации по ВОЛС С ≤ 500 Мбит/с, то преобладающими шумами цифрового фотоприемника являются дробовые шумы с пуассоновской статистикой, а для скоростей передачи информации по ВОЛС С ≤ 500 Мбит/с, преобладающими шумами цифрового фотоприемника являются тепловые шумы с гауссовской статистикой [7].

При обнаружении информационных сигналов на фоне шумов применяют критерий Неймана-Пирсона. Согласно критерию Неймана-Пирсона, фотоприемник является оптимальным в том случае, если при заданной вероятности ложной тревоги, он обеспечивает максимальную вероятность обнаружения информационного сигнала.

Выбор порогового значения вероятности обнаружения информационного сигнала целесообразно осуществлять с точки зрения минимизации вероятности ошибки $P_{ош}$, которая рассчитывается по формуле [8]:

$$P_{ош} = 0{,}5 \times (1 - P_0 + P_{лт}),$$

где P_0 – вероятность обнаружения информационного сигнала;

$P_{лт}$ – вероятность ложной тревоги.

Случай, когда вероятность ошибки соизмерима с вероятностью обнаружения обнаружения информационного сигнала, является случаем наибольшей неопределенности при принятии решения о наличии или отсутствии информационного сигнала. Поэтому в качестве порогового значения вероятности обнаружения целесообразно принять $P_0 \approx 0{,}3$.

Как правило, для обеспечения достаточной для инженерных расчетов точности ошибка измерения не должна превышать 10 % от значения вычисляемой величины.

Следовательно, в качестве порогового значения вероятности обнаружения целесообразно принять $P_0 \approx 0{,}8$

В качестве критерия эффективности защиты следует считать значения вероятностей обнаружения информационного сигнала, приведенные в таблице 1 [9].

Таблица 1

Задача технической защиты информации	Критерий эффективности защиты
Полное скрытие информационных сигналов, которые возникают при обработке информации или ведении переговоров (скрытие факта обработки информации ограниченного распространения на объекте)	$P_0 \leq 0{,}3$
Скрытие параметров информационных сигналов, которые возникают при обработке информации или ведении переговоров, по которым можно восстановить информацию ограниченного распространения (скрытие информации, обрабатываемой на объекте)	$P_0 \leq 0{,}8$

В случае слабого информационного сигнала и интенсивных помех число фотоотсчетов в принимаемой реализации смеси информационного сигнала и шума должно быть достаточно большим. Лишь в этом случае можно осуществить уверенный прием и выделить полезный информационный сигнал.

Вероятность ложной тревоги и вероятность обнаружения информационного сигнала определяются следующим образом [10]:

$$\mathrm{P}_{\text{лт}} = 1 - \Phi\left(\frac{\lambda_0 - m_1}{\sigma_1}\right), \quad (1)$$

$$\mathrm{P}_{\text{лт}} = 1 - \Phi\left(\frac{\lambda_0 - m_2}{\sigma_2}\right), \quad (2)$$

где λ_0 – отношение правдоподобия;

$\Phi(t) = \frac{1}{\sqrt{2 \cdot \pi}} \cdot \int_{-\infty}^{t} \exp\left(-\frac{x^2}{2}\right) dx$ – интеграл вероятности.

В том случае, когда статистики сигнальных и шумовых фотоэлектронов являются пуассоновскими, то

$$m_1 = N \cdot \left(a_0 < s_{\text{ш}} >\right) - b_0, \qquad \sigma_1^2 = N \cdot a_0^2 < s_{\text{ш}} >,$$

$$m_2 = N \cdot \left[a_0 \cdot \left(< s_{\text{с}} > + < s_{\text{ш}} >\right) - b_0\right], \qquad \sigma_2^2 = N \cdot a_0^2 \cdot \left(< s_{\text{с}} > + < s_{\text{ш}} >\right),$$

$$a_0 = \frac{< s_{\text{с}} >}{< s_{\text{ш}} >}, \qquad b_0 = < s_{\text{с}} >,$$

где N – число фотоотсчетов;

$< s_{\text{с}} >$ – средняя энергия сигнальных фотоэлектронов;

$< s_{\text{ш}} >$ средняя энергия шумовых фотоэлектронов.

Если статистика сигнальных фотоэлектронов является пуассоновской, а шумовых фотоэелектронов – гауссовской, то

$$m_1 = \delta_0 \cdot N \cdot \frac{< s_{\text{ш}} >}{1 + < s_{\text{ш}} >}, \qquad \sigma_1^2 = \delta_0^2 \cdot N \cdot \frac{< s_{\text{ш}} >}{1 + < s_{\text{ш}} >},$$

$$m_2 = \delta_0 \cdot N \cdot \frac{< s_{\text{ш}} >}{1 + < s_{\text{ш}} >}, \qquad \sigma_2^2 = \delta_0^2 \cdot N \cdot \frac{2 \cdot < s_{\text{с}} > \cdot < s_{\text{ш}} > + < s_{\text{с}} > + \left(< s_{\text{ш}} >\right)^2 + < s_{\text{ш}} >}{\left(1 + < s_{\text{ш}} >\right)^2}.$$

Предельно допустимое (пороговое) значение отношения сигнал/шум на входе в фотоприемник получим, решив уравнения (1) и (2) относительно δ_0.

Список литературы

1. Ветохин, С. С. Одноэлектронные фотоприемники / С. С.Ветохин, И. Р. Гулаков, А. Н. Перцев – М. : Энергоатомиздат, 1986. – 246 с.

2. Гудмен, Дж. Статистическая оптика / Дж. Гудмен. – М. : Мир, 1988. – 528 с.

3. Матвеев, И. Н. Лазерная локация / И. Н.Матвеев [и др.] ; под ред. Н. Д. Устинова. – М. : Машиностроение, 1984. – 272 с.

4. Клаудер, Дж. Основы квантовой оптики / Дж. Клаудер, Э. Сударшан. – М. : Мир, 1970. – 430 с.

5. Александров, С. Е. Влияние низкочастотных шумов на пороговую чувствительность фотодиодных фотоприемных устройств среднего ИК-диапазона в широкой полосе частот / С. Е. Александров, Г. А. Гаврилов, Г. Ю. Сотникова // Письма в ЖТФ. – 2014. – Т. 40, вып. 16. – С. 58–64.

6. Торшина, И. П. Выбор приемника излучения при проектировании оптикоэлектронного прибора : учеб. пособие / И. П.Торшина, Ю. Г. Якушенков. – М. : Изд-во МИИГАиК, 2017. – 58 с.

7. Шубин, В. В. Информационная безопасность волоконно-оптических систем / В. В. Шубин. – Саров : РФЯЦ-ВНИИЭФ, 2015. – 257 с.

8. Хорев, А. А. Теоретические основы оценки возможностей технических средств разведки / А. А. Хорев. – М. : МО РФ, 2000. – 255 с.

9. Хорев, А. А. Оценка эффективности защиты информации от утечки по техническим каналам / А. А. Хорев // Специальная техника. – 2006. – № 6. – 53–61.

10. Шереметьев, А. Г. Статистическая теория лазерной связи / А. Г. Шереметьев. – М. : Связь, 1971. – 264 с.

УДК 004.056.53

МЕТОДЫ АНАЛИЗА РИСКОВ СОЦИОИНЖЕНЕРНЫХ АТАК НА КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ РАЗЛИЧНОЙ СЛОЖНОСТИ

А.Г. ДАВЫДОВСКИЙ
Учреждение обучения «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Введение. Понятие «киберфизические системы» (от англ. cyber-physical systems, или CPS) основано на представлении о комплексных системах, включающих вычислительные и физические элементы, которые постоянно получают данные из окружающей среды и используют их для дальнейшей оптимизации процессов управления. В киберфизических системах осуществляется интегральное взаимодействие между вычислительными, виртуальными процессами и процессами физическими, реальными. К киберфизическим системам можно отнести «умный дом», «умное предприятие», «умную дорогу», «умный регион», «умные» сети электроснабжения, системы управления «умным» транспортом, автоматизированные системы управления в производстве, сельском хозяйстве, медицин. Одним из примеров киберфизических систем являются такие масштабные и комплексные социотехнические решения, как «умные города» [1].

Одной из важных проблем для развития киберфизических систем и технологий, основанных на их применении, является непрерывный рост числа киберпреступлений (социоинженерных атак – СИА), совершаемых с применением методов социальной инженерии в отношении критически важных информационных ресурсов, связанных с киберфизическими системами различного масштаба и назначения. СИА включают набор прикладных психологических и аналитических приемов, которые злоумышленники применяют для скрытой мотивации пользователей публичной или корпоративной сети к нарушениям устоявшихся правил и политик в области информационной безопасности [2, 3].

Проблема защиты пользователей персонала и пользователей КФС от СИА чрезвычайно актуальна в настоящее время. Вместе с тем, основные исследования в области информационной безопасности посвящены вопросам защиты информационных систем от программно-технических атак, но не от СИА [3, 4]. В настоящее время остаются недостаточно разработанными различные аспекты моделирования, прогнозирования и превентивного управления рисками развития социоинженерных атак на КФС и их пользователей [5].

Цель данной статьи – характеристика методов анализа рисков социоинженерных атак на киберфизические системы различной сложности, включая метод экспертных оценок и методы математического моделирования.

Методы экспертных оценок рисков социоинженерных атак. Под СИА принято понимать совокупность действий злоумышленника, направленную на другое лицо (или группу лиц) с целью достижения желаемого результата, в частности, нарушения безопасности информации (организации доступа к информации, передача ее другому лицу и т. п.) [6]. СИА могут быть рассмотрены как вид информационно-психологических воздействий, оказывающих влияние на восприятие человеком реальной действительности, в частности на его поведенческие функции [7]. Под гибридными СИА здесь предложено понимать комплекс атакующих воздействий, так изменяющих состояние антропогенных (пользователи, персонал), квазиантропогенных (искусственный или гибридный интеллект), программно-технических, инфраструктурных, производственных и экологических компонентов КФС, когда нарушается функционирование этой системы, а часто становится невозможным само ее существование в ближайшей или отдаленной перспективе. Каждый из перечисленных факторов может быть подвергнут декомпозиции с выделением еще более элементарных составляющих. Злоумышленники, обладающие навыками социоинженеров, с легкостью могут повлиять на персонал или пользователей КФС через каналы коммуникаций с внешней средой с последующим нарушением или дезинтеграцией системы, имеют различные уязвимости, степень их выраженности может различаться. В этом

случае целесообразно рассматривать профиль уязвимостей как модель (разной степени полноты и завершенности) системы всех уязвимостей пользователя. Основу уязвимости может составлять ряд психологических особенностей, равно как и одна и та же психологическая особенность может обеспечивать различные уязвимости [8].

Важную роль в оценке рисков СИА и степени тяжести их последствий играют методы экспертных оценок с использованием эвристических методов прогнозирования, которые возможно применять как в качестве самостоятельных технологий прогнозирования, так и в качестве дополнения к формальным методам. При разработке прогнозов рисков СИА целесообразно использовать оптимизированные модели прогнозной оценки развития предприятия с использованием экспертных технологий, состоящая из следующих этапов:

–определение средней оценки из оценок экспертов с использованием различных критериев оптимизации для каждому потенциальному социотехническому фактору формирования риска социоинженерных атак на КФС;

–расчет средней оценки характеристик, относящихся к конкретному подуровню КФС;

–расчет средней оценки уровня состояния КФС по направлению системного анализа ее функционирования;

–расчет средней оценки уровня текущего состояния КФС в целом.

Для характеристики надежности КФС предложена модель функции желательности. На основе численного моделирования установлены пять диапазонов риска нарушения функционирования КФС ($R_{КФС}$) при гибридных СИА (в баллах от 0 до 100): низкий ($0 \le R_{КФС} \le 20$), допустимый ($20 \le R_{КФС} \le 37$), средний ($37 \le R_{КФС} \le 63$), высокий ($63 \le R_{КФС} \le 80$) и критический ($80 \le R_{КФС} \le 100$).

Оценка вероятности СИА ($P_{СИА}$) и их последствий для КФС ($W_{КФС}$) является сложной задачей и может быть успешно решена с использованием инструментария экспертных оценок для комплекса показателей КСФ, включая количество входящих в ее состав компонентов (N), число иерархических уровней (L), количество связей между системой и внешней средой (C). По каждому показателю формируются матрицы прогнозируемых показателей в зависимости от многих трудноуправляемых факторов $f_1, f_2., \ldots, f_n$:

$$\left\| Risk_n(f_1, f_2, ..., f_i) \right\| \tag{1}$$

Формирование происходит по каждому из социотехнических факторов риска развития СИА. Данные показатели выступают как показатели эффективности Э (f_1, f_2., …, fn) функционирования КФС. На основе компаративного анализа различных вариантов композиций таких трудноуправляемых факторов отбираются только наименее и наиболее благоприятные варианты. В дальнейшем используется принцип оптимальности (принцип оптимизма, пессимизма, гарантированного результата или принцип Сэвиджа):

$$Э = \max_{f_1 \in F'} \min_{f_2 \in F} Э(f_1, f_2), \tag{2}$$

где F – совокупность внешнесредовых факторов, оказывающих влияние на прогнозируемые показатели;

F' – совокупность альтернативных управленческих решений, из которых принимается наиболее эффективное.

Моделирование и прогнозирование рисков социоинженерных атак на основе социотехнического подхода. В любой КФС можно выделить инвариантные (неизменяемые, базовые) и вариативные (изменяемые) структурно-функциональные элементы (N). К инвариантным элементам относятся антропогенные (люди, пользователи, персонал), квазиантропогенные (системы поддержки принятия решений, искусственного (или гибридного) интеллекта), технологии, инфраструктуры, коммуникации, институциональные и внешнесредовые компоненты. КФС имеют структурно-функциональные уровни (L), от 3 до 12 (чаще всего, от 3 до 7), а также связи с внешней средой (C). При этом внешняя среда характеризуется наличием угроз различного масштаба, которые воздействуют на КФС с определенной

интенсивностью (Λ) . При этом наиболее адекватным для моделирования и прогнозирования рисков социоинженерных атак является социотехнический подход.

Полагая, что удельная плотность коммуникаций с внешней средой пропорциональна удельной плотности элементов по иерархическим уровням, можно охарактеризовать информационный потенциал КФС (I):

$$I = \frac{C \cdot L}{N}, \tag{3}$$

Очевидно, что такие внешние воздействия в сочетании со сложностью и уязвимостью внутренней организации КФС определяют вероятность аварийных отказов и аварий (A) в КФС:

$$\frac{dA}{dt} = \left(1 + a_1\Lambda + f_1 I - g_1 P\right)A. \tag{4}$$

Вместе с тем, надежность КФС может быть выражена как:

$$\frac{dP}{dt} = \left(1 - a_1\Lambda - f_2 I - g_2 A\right)P. \tag{5}$$

В уравнениях (4) – (5) предусмотрена возможность взаимного влияния факторов, которые определяют уязвимость КФС для кибератак, либо устойчивость к ним. Эти два уравнения позволяют получить условие устойчивости КФС в неустойчивой внешней среде, являющейся источником разнообразных гибридных СИА:

$$\frac{dP}{dt} - \frac{dA}{dt} = \begin{cases} > 0 & - \text{ надежное, устойчивое состояние КФС;} \\ \to 0 & - \text{ неустойчивое состояние и угроза дезинтеграции;} \\ < 0 & - \text{ потеря надежности и развитие дезинтеграции КФС.} \end{cases} \tag{6}$$

Разделив уравнения (4) и (5) друг на друга, после несложных преобразований и интегрирования по частям, можно получить уравнение, связывающее вероятность снижения устойчивости и надежность КФС в условиях гибридных СИА:

$$\ln A - \ln P - g_2 A + g_1 P - \int_0^{+\infty} \frac{dA}{A}\left(\left(a_2\Lambda + f_2 I\right)\right) - \int_0^{+\infty} \frac{dP}{P}\left(\left(a_1\Lambda + f_2 I\right)\right) = C, \tag{7}$$

где С – постоянная.

Анализ данного уравнения и, в частности, его члена $\left(a_1\Lambda + f_2 I\right)$, обусловливает сопряженное и однонаправленное влияние интенсивности угрожающих событий и удельной плотности коммуникаций в иерархии КФС. По сути, избыточное количество связей КФС с внешней средой может оказывать такое же влияние на надежность КФС, как и угрозы, исходящие из внешней социотехнической среды.

Кроме того, в рамках социотехнического подхода может быть успешно использован метод сценарного моделирования.

Множественное линейное регрессионное моделирование для анализа рисков социотехнических атак. В условиях социально-гуманитарных катастроф вероятность СИА существенно возрастает, также, как и тяжесть их последствий. Примеров такой социально-гуманитарной катастрофы является пандемия COVID-19. В этих условиях уязвимость персонала и пользователей КФС существенно возрастает. Причем медийные факторы, тренды и приоритеты в социальных сетях Интернет могут быть теснейшим образом связаны с реальными социальными и эпедимологическими событиями.

В этой связи была изучена взаимосвязь и оценено возможное влияние тематических обращений пользователей Интернет-ресурсов на динамику новых случаев заболевания COVID-19 на основе метода множественного линейного регрессионного анализа.

В используемой модели линейной регрессии в качестве объясняемых (зависимых) переменных рассмотрены Y_1 «новые случаи заболевания», Y_2 «накопление случаев заболева-

ния», Y_3 «новые случаи смерти» и Y_4 «накопление новых случаев смерти», а в качестве факторов-регрессоров (независимых переменных) – лингвистические переменные, выделенные из лексического пространства сообщений на новостных Интернет-порталах, посвященных последствиям пандемии COVID-19, такие как X_i «covid-19», «ковид», «медицинские перчатки», «медицинские маски», «вакцина против COVID-19», «самоизоляция», «карантин», «дистанционное обучение», «Википедия» [9]. Для выделения лингвистических переменных из лексического пространства сообщений по COVID-19 были использованы модифицированные метрики Евклида и Махаланобиса [10]. Оценка степени соответствия на соответствие нормальному распределению временных рядов показателей обращений пользователей на различных Интернет-ресурсах был осуществлена с использованием критериев Колмогорова-Смирнова, Лилиефорса и Шапиро-Уилка. Были получены четыре линейные множественные регрессионные модели влияния тематических обращений пользователей Интернет на динамику новых случаев заболевания COVID-19 (8) – (11):

$$Y_{1\,(\text{новые случаи заболевания})} = 54{,}1X_1 + 123{,}8X_2 + 404{,}7X_3 - 44{,}1X_4 + 1367{,}9X_5 - \\ - 391{,}5X_6 - 17{,}6X_7 - 117{,}7X_8 + 11{,}9X_9 \ (R^2 = 0{,}81); \quad (8)$$

$$Y_{2\,(\text{накопление случаев заболевания})} = -7479{,}7X_1 + 10938{,}2X_2 + 78043{,}5X_3 - 12591{,}0X_4 + \\ + 389625{,}9X_5 + 65450{,}5X_6 - 1347{,}8X_7 - 19054{,}5X_8 + 5528{,}2X_9 \ (R^2 = 0{,}83); \quad (9)$$

$$Y_{3\,(\text{новые случаи смерти})} = 0{,}17X_1 + 0{,}49X_2 + 2{,}31X_3 - 0{,}92X_4 + 9{,}6X_5 + 4{,}41X_6 - 0{,}14X_7 - \\ - 1{,}82X_8 + 0{,}32X_9 \ (R^2 = 0{,}87); \quad (10)$$

$$Y_{4\,(\text{накопление случаев смерти})} = -79{,}6X_1 + 91{,}6X_2 + 634{,}0X_3 - 92{,}1X_4 + 2339{,}4X_5 + \\ + 524{,}2X_6 - 6{,}65X_7 - 47{,}9X_8 + 41{,}9X_9 \ (R^2 = 0{,}85). \quad (11)$$

Анализ регрессионных моделей (8) – (11) позволяет выделить ключевые инфоповоды-драйверы, изменение которых сопровождается превентивным управлением динамикой новых случаев заболевания, накопления случаев заболевания, новых случаев смерти и накопления случаев смерти при COVID-19, а также других социальных процессов в реальном мире [11, 12].

Заключение. Таким образом, предложенные модели могут быть рекомендованы для оценки текущего состояния и тенденций развития КФС, в частности, в условиях пандемии COVID-19, с помощью своременных методов и технологий прогнозирования. Результаты моделирования и прогнозирования надежности КФС в условиях гибридных СИА могут стать основанием как для принятия управленческих решений, так и для разработки аналогичных прогнозов другими методами. В моделировании социоинженерного воздействия важное значение имеет выявления предрасположенности пользователей к информационному воздействию в зависимости от места и роли субъекта в социальной структуре. В этой связи актуальной проблемой является разработка комплекса комбинированных статистических, лингвистических и логико-стохастических моделей и программного инструментария для прогнозирования и превентивного управления рисками и сценариями развития СИА на пользователей КФС как компонентов социотехнических комплексов на разных стадиях их жизненного цикла на основе подходов наибольшего правдоподобия, логико-вероятностного анализа и сценарного моделирования рисков развития негативных последствий цифровых трансформаций различных областей социальной практики, социоинженерной активности, киберпреступности и высокотехнологического терроризма в условиях четвертой промышленной революции [11, 12].

Список литературы

1. Ястреб, Н. А. Индустрия 4.0: киберфизические системы, разумное окружение, Интернет вещей / Н. А. Ястреб. – [Электронный ресурс]. – Режим доступа : https://techno.vogu35.ru/docs/2015/Industria_4_0_Yastreb.pdf . – Дата доступа : 12.03.2021.

2. Опасности цифровизации или цифровизация в опасности // Digital Forum РБК. – [Электронный ресурс]. – Режим доступа : https://spb.plus.rbc.ru/news/5cb448c57a8aa90a3814c68e. – Дата доступа : 19.05.2019.

3. Asim, M. AndroKit: A toolkit for forensics analysis of web browsers on android platform / M. Asim // Future Generation Computer Systems. – 2019.

4. Li, H. Self-control, organizational context, and rational choice in Internet abuses at work / H. Li [et al.] // Information & Management. – 2018.

5. Митник, К. Д. Искусство обмана / К. Д. Митник, В. Л. Саймон. – М. : Компания АйТи, 2004.

6. Абрамов, М. В. Психологические особенности, психические состояния пользователя и профиль его уязвимостей в контексте социоинженерных атак [Электронный ресурс] / М. В. Абрамов, А. Л. Тулупьев, Т. В. Тулупьева. – Режим доступа : https://dspace.kpfu.ru/xmlui/bitstream/handle/net/151044/F_zpsh2019_ 312_317.pdf?sequence=-1. – Дата доступа : 12.04.2021.

7. Баришполец, В. А. Информационно-психологическая безопасность: основные положения / В. А. Баришполец // Информационные технологии. – 2003.

8. Тулупьев, А. Л. Психологические особенности персонала, предрасполагающие к успешной реализации социоинженерных атак / А. Л. Тулупьев [и др.] //Научные труды Северо-Западного института управления. – 2012.

9. Себер, Дж. Линейный регрессионный анализ / Дж. Себер. – М. : Мир, 1980.

10. Гельфанд, И. М. Лекции по линейной алгебре / И. М. Гельфанд. – М. : Добросвет, МЦНМО, 1998.

11. Davidovsky, A. G. The Problem of Preventive Management of Technological Risks in the Industry 4.0 / A. G. Davidovsky // European Sciences Review. – 2019.

12. Хлобыстова, А. О. Подход наибольшего правдоподобия к задаче выявления траекторий социоинженерных атак и скомпрометированных пользователей информационных систем / А. О. Хлобыстова, М. В. Абрамов, А. Л. Тулупьев // Системы управления, связи и безопасности. – 2019.

УДК 004

АНАЛИЗ ПРИНЦИПОВ РАБОТЫ СЕТИ ПРИ ОДНОНАПРАВЛЕННОЙ ПЕРЕДАЧЕ ДАННЫХ В КОМПЬЮТЕРНЫХ СЕТЯХ

Р.А. РУМАС[1], Ю.В. ВОРОТНИЦКИЙ[2]
[1]*Оперативно-аналитический центр при Президенте Республики Беларусь, г. Минск, Республика Беларусь*
[2]*Белорусский государственный университет, г. Минск, Республика Беларусь*

Однонаправленная передача данных предполагает, что устройство в компьютерных сетях может только передавать данные или только получать их. При этом устройство – источник данных может осуществлять их передачу одному или нескольким устройствам – приемникам, но последние не могут передавать данные источнику. Однонаправленная передача данных применяется для безопасной передачи информации, например, файлов, журналов событий, почтовых сообщений, промышленных протоколов, обновлений программного обеспечения.

Задача однонаправленной передачи данных затрагивает различные уровни эталонной модели взаимодействия открытых систем (Open System Interconnection, OSI) [1].

Известны решения (например, [2]), в которых однонаправленная передача данных обеспечивается путем гальванической развязки источника и приемника. Например, можно создать однонаправленный канал передачи данных на физическом уровне с помощью дуплексного волоконно-оптического соединения, которое должно использовать два волоконно-оптических кабеля: один для передачи и один для приема сигнала (рис. 1), отключив одно из этих соединений. В этом случае устройства будут взаимодействовать только в одном направлении.

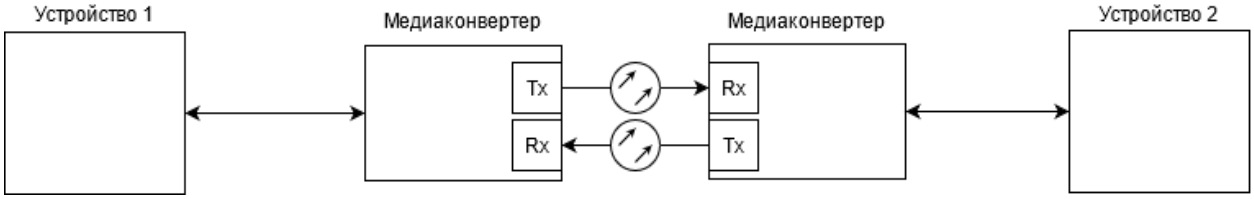


Рис. 1. Двустороннее волоконно-оптическое соединение

Для работы на канальном уровне модели OSI компьютерам необходимо адресовать пакеты согласно уникальным идентификаторам, называемыми MAC-адресами (Media Access Control). Предварительно по протоколу ARP (Address Resolution Protocol) необходимо обменяться информацией для установления соответствия MAC-адреса и IP-адреса компьютера, с которым необходимо взаимодействовать [3]. Однако при однонаправленном канале передачи данных обмен информацией произведен не будет. Одним из способов решения данной проблемы является установление статического соответствия MAC-адреса и IP-адреса на компьютере-отправителе.

Для работы на сетевом и транспортном уровнях модели взаимодействия OSI при однонаправленной передаче данных необходимо использовать протоколы без установления логической связи, которая подразумевает двунаправленное взаимодействие. Протокол IP на сетевом уровне является протоколом без установления логической связи [4]. При использовании транспортных протоколов следует выбрать UDP, который является дейтаграммным протоколом, реализующим так называемый ненадежный сервис по возможности, который не гарантирует доставку сообщений адресату, но обеспечивающий работу без необходимости предварительного сообщения для установки специальных каналов передачи [5]. Для реализации передачи данных можно воспользоваться, например, Unix утилитой NetCat, позволяющая устанавливать соединения TCP и UDP, принимать данные и передавать их [6].

Для создания интерфейсов между компьютерными устройствами и системой однонаправленной передачи данных могут использоваться специализированные прокси-сервера [2],

обеспечивающие преобразование двусторонних протоколов в односторонние на передающей стороне, односторонних в двусторонние – на принимающей и организующие однонаправленный транспорт между собой (рис. 2).

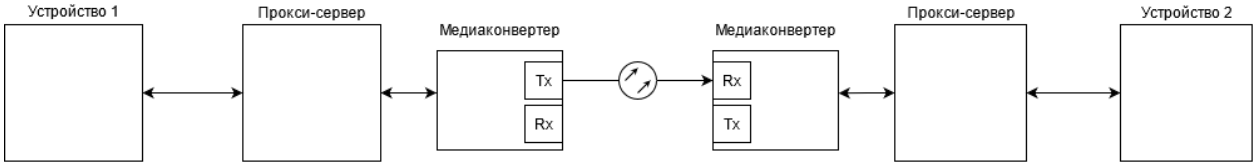


Рис. 2. Архитектура одностороннего соединения

Можно сделать вывод, что методика проектирования программно-аппаратного средства однонаправленной передачи данных, которое будет удовлетворять конкретным требованиям по обеспечению целостности, доступности и конфиденциальности информационных ресурсов в тех или иных объектах информатизации, должна включать в себя реализацию комплекса необходимых решений на различных уровнях эталонной модели и предполагает разработку соответствующих алгоритмов однонаправленной передачи данных, реализуемых программным путем.

Список литературы

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учеб. пособие для студ. вузов / В. Г. Олифер, Н. А. Олифер. – 4-е изд. –М. ; СПБ. ; Н. Новгород [и др.] : Питер, 2010. – 944 с.

2. АПК АМТ InfoDiode – Система однонаправленной передачи данных [Электронный ресурс]. – Режим доступа : http://amt.ru/web/ru/infodiode. – Дата доступа : 20.04.2021

3. RFC 826: Address Resolution Protocol [Электронный ресурс]. – Режим доступа : https://www.ietf.org/rfc /rfc0826.txt. – Дата доступа : 20.04.2021.

4. RFC 791: Internet Protocol [Электронный ресурс]. – Режим доступа: https://www.ietf.org/rfc/rfc0791.txt. – Дата доступа : 20.04.2021.

5. RFC 768: User Datagram Protocol [Электронный ресурс]. – Режим доступа: https://www.ietf.org/rfc/rfc0768.txt. – Дата доступа : 20.04.2021.

6. The GNU Netcat Project [Электронный ресурс]. – Режим доступа: http://netcat.sourceforge.net/. – Дата доступа : 20.04.2021.

ЗАСЕДАНИЕ № 7
ШКОЛА МОЛОДЫХ УЧЕНЫХ

УДК 004.942

РАЗВИТИЕ СИСТЕМЫ ЗАЩИТЫ ДЛЯ ПЛАТФОРМЫ ВИРТУАЛИЗАЦИИ

И.В. ЧУМАКОВ, Н.В. МОЗОЛИНА
МФТИ (НИУ), г. Москва, Российская Федерация
ЗАО «ОКБ САПР», г. Москва, Российская Федерация

Введение. К настоящему времени про виртуализацию слышал каждый, и многим известны ее преимущества: гибкое управления инфраструктурой, эффективное энергосбережение, отказоустойчивость и многое другое. Уже ни для кого не секрет, что множество компаний уже используют облака в своей IT-инфраструктуре, и этот тренд продолжается [1]. Такая популярность технологии ожидаемо привлекает внимание специалистов по информационной безопасности к созданию новых и модернизации уже существующих решений.

VMware уже 20 лет разрабатывает решения для серверной виртуализации и за это время стала лидером на рынке. Платформа VMware vSphere используется во многих информационных системах, обрабатывающих данные, требующие защиты. Поэтому и для защиты виртуальной инфраструктуры VMware представлено множество средств защиты информации, например, компанией ОКБ САПР были разработаны два продукта: Аккорд-В. и Сегмент-В. [2]. Платформа виртуализация VMware vSphere продолжает развиваться, среди специалистов по защите информации происходит переосмысление принципов построения СЗИ, в том числе и СЗИ для виртуальных инфраструктур.

В данном докладе будут представлены результаты исследования, направленного на построение системы защиты виртуальной инфраструктуры на базе VMware vSphere 6.7 в соответствии с современными требованиями [3–5].

Исследование ограничивается рассмотрением мер защиты, связанных с обеспечением целостности объектов ВИ, управлением миграциями, сегментированием виртуальной инфраструктуры и управлением доступом администраторов ВИ к ее объектам. Прочие требования к СЗИ для систем виртуализации на данном этапе работы не рассматривались.

Объектом исследования стала виртуальная инфраструктура, построенная на базе платформы VMware vSphere 6.7.

Как построить систему защиты виртуальной инфраструктуры? В соответствии с [4, 5] система защиты должна обеспечивать защищенность всех компонентов среды виртуализации: ESXi-серверов и самих виртуальных машин, серверов управления vCenter, выполненных в виде как виртуальных машин (VCSA), так и специального программного обеспечения для Windows Server. Для этого в состав системы должно входить СЗИ, позволяющее осуществить доверенную загрузку, контроль целостности этих объектов и доступа к ним.

Рассмотрим каждый из этих объектов и сформулируем требования к СЗИ, позволяющему обеспечить их защищенность.

Основным компонентом в системе виртуализации vSphere является ESXi-сервер – гипервизор, компонент, который обеспечивает функционирование виртуальных машин, а также осуществляет управление ими. Компрометация любого компонента ESXi может привести к компрометации всех работающих на нем виртуальных машин, а, следовательно, и данных, которые ими обрабатываются. Поэтому крайне важно обеспечить доверенную загрузку ESXi-серверов и пошаговый контроль целостности всех его компонентов. Также ESXi можно рассмотривать как специализированную операционную систему, управление которой может осуществляться локально, через терминал администраторами виртуальной инфраструктуры, а значит, необходимо осуществлять идентификацию и аутентификацию локальных администраторов гипервизора.

Другим объектом ВИ, защита которого необходима (именно на нем выполняется обработка и хранение данных) является виртуальная машина. Виртуальным машинам присущи все те же угрозы, что и их «реальным» аналогам. Для них точно так же необходимо обеспечивать доверенную загрузку и контроль целостности файлов внутри виртуальной машины. Список контролируемых СЗИ компонентов виртуальных машин, которыми могут быть BIOS, главная загрузочная запись (MBR) жестких дисков, оборудование, и файлы [6], должен быть настраиваемым и определяться администратором безопасности в соответствии с политикой безопасности компании, владеющей виртуальной инфраструктурой.

При назначении контролируемых файлов для однотипных виртуальных машин удобно использовать файл-лист – единый список, в котором будут заданы параметры контролируемых файлов ВМ. Идея такого списка уже была реализована в Аккорд-KVM [7] и успешно показала себя. Этот список содержит перечень полных путей к контролируемым файлам и их контрольные суммы, рассчитанные на основании файлов эталонной ВМ. В последствии такой файл-лист может быть назначен однотипным виртуальным машинам (подобным эталонной) и при выполнении процедуры проверки контрольные суммы файлов ВМ сравниваются с указанными в файл-листе. В средстве защиты для ВИ, построенных на базе VMware vSphere, как и для инфраструктур, построенных на базе гипервизора KVM, целесообразно предусмотреть именно такую реализацию контроля целостности файлов ВМ.

Еще одним объектом, составляющим ВИ, является сервер управления виртуальной инфраструктурой, vCenter Server. В случае его реализации как виртуальной машины, его защита должна осуществлять аналогично и другим ВМ, а случае реализации как физического СВТ – аналогично другим физическим СВТ. В первом случае безопасность vCenter может быть обеспечена СЗИ для ВИ, установленного в той же инфраструктуре, что и сервер управления. Во втором случае обеспечение безопасности vCenter как физического СВТ должно осуществляться средством доверенной загрузки, например, Аккорд-АМДЗ [8], и СЗИ от НСД, например, СПО Аккорд-Win64 K [9].

Теперь рассмотрим требования к обеспечению мер защиты, связанных с миграциями ВМ и сегментированию ВИ.

Миграция и сегментирование неразрывно связаны между собой. С одной стороны, выделение сегментов ВИ подразумевает ограничение на перемещение ВМ, то есть их миграцию между хостами, принадлежащих разным сегментам. С другой стороны, контроль миграции позволяет разделить объекты ВИ на группы, то есть выполнить сегментирование.

Контроль миграции ВМ должен позволить ограничить список гипервизоров, ресурсы которых могут быть использованы данной виртуальной машиной. Иными словами, СЗИ должно разрешать или блокировать запуск ВМ на ESXi-серверах в зависимости от заданных администратором безопасности настроек миграции.

Конечно, контроль перемещения виртуальных машин между ESXi-серверами позволяет выделить в ВИ группы ее объектов, но лишь группы виртуальных машин и гипервизоров. Виртуальные сети, хранилища и другие компоненты ВИ при таком построении системы защиты не рассматриваются. В то время как для полноценного выполнения требования сегментирования необходимо учитывать и эти объекты. Следовательно, СЗИ должно осуществлять контроль перемещений объектов всех типов, существующих в ВИ.

Далее перейдем к вопросу об управлении доступом администраторов ВИ к ее объектам. При использовании для разграничения доступа лишь встроенных механизмов VMware vSphere возникает проблема сосредоточения максимальных привилегий в рамках одной роли главного администратора ВИ, то есть проблема «суперпользователя» [10]. Такой администратор может назначить любые права любому пользователю, дать доступ к любому объекту, являясь при этом администратором ВИ, а не безопасности – в рамках одного пользователя сосредоточены права двух администраторов, каждый из которых должен решать свои задачи и преследовать свои интересы. Хотя решить данную проблему зачастую возможно организационными мерами, это не всегда удобно. Хотелось бы администратору безопасности самому разрешать пользователям выполнение только определенных действий, не являясь при этом администратором ВИ. Такое разделение полномочий администратора безопасности и администратора ВИ позволяет решить проблему «суперпользователя».

Рассмотрев требования к защите основных объектов виртуальной инфраструктуры, перейдем к выработке требования к архитектуре СЗИ.

Управление системой защиты удобно осуществлять централизованно, например, каждый администратор безопасности со своего АРМ подключается через консоль управления к серверу управления виртуальной инфраструктурой. Доступ к инструментам управления системой защиты должен быть только у администраторов безопасности, от администраторов виртуальной инфраструктуры эти инструменты должны быть скрыты.

При всем этом система защиты не должна в целях безопасности ограничивать возможностей виртуальной инфраструктуры, сводя их к минимуму. Все преимущества систем виртуализации должны оставаться доступными.

Стоит отметить, что вне зависимости от функции безопасности, осуществляемых СЗИ, крайне важно, чтобы СЗИ обладало свойством отказоустойчивости.

Как реализовать требования к защите на примере Аккорд-В. 2.0?

Практическим результатом выполненной научно-технической работы стало создание макета программы Аккорд-В. 2.0. Это специальной программное обеспечение позволяет выполнить требования к СЗИ для защиты виртуальной инфраструктуры, указанные выше, а также является развитием продуктов ОКБ САПР Аккорд-В. 1.3 и Сегмент-В. 1.3. Архитектура Аккорд-В. 2.0 и связи между его компонентами представлены на рисунке 1.

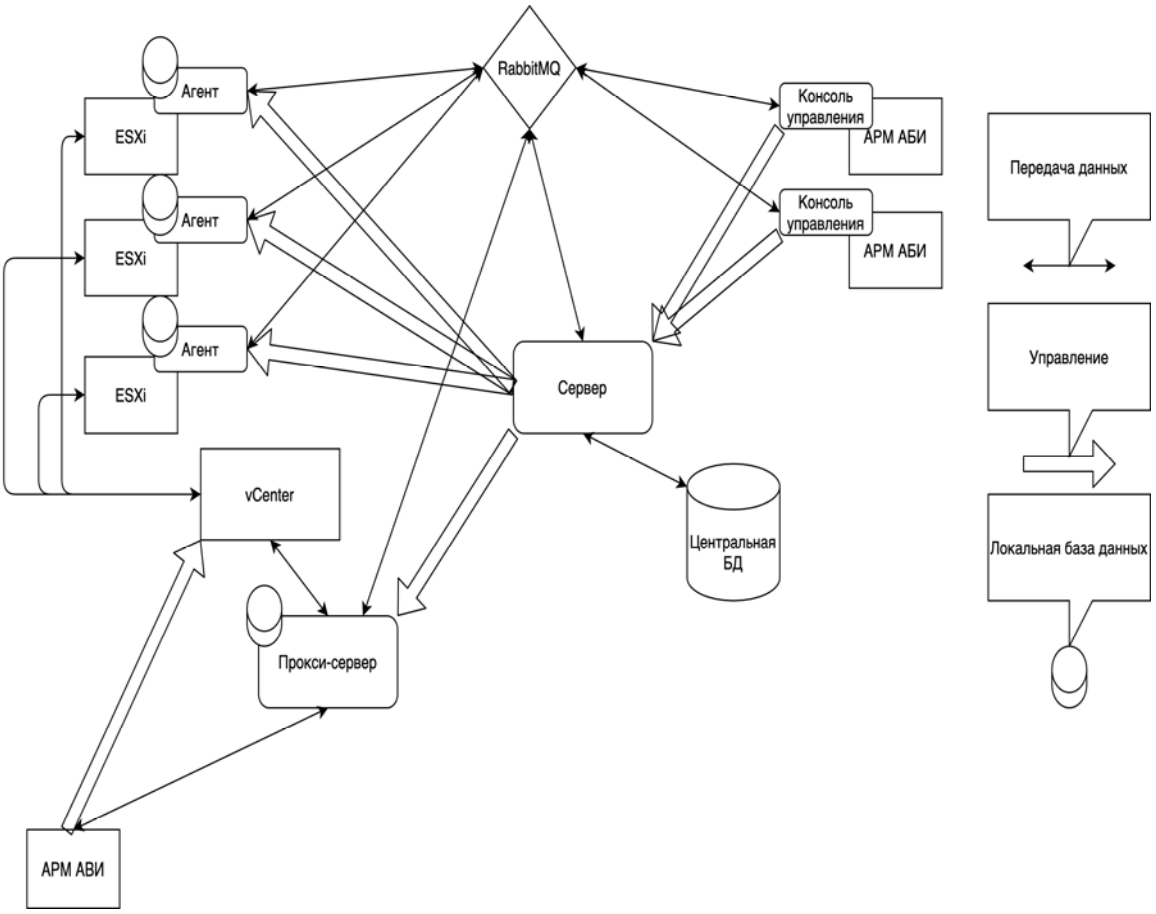


Рис. 1. Архитектура СПО «Аккорд-В

Аккорд-В. 2.0 состоит из следующих компонентов:

• Агенты – это программные модули, которые работают на ESXi-серверах и осуществляют доверенную загрузку виртуальных машин, а также контролируют миграции ВМ;

• Прокси-сервер – это программный модуль, работающий на отдельном сервере и обрабатывающий поступающие запросы от АРМ администратора виртуальной инфраструктуры к vCenter;

• Консоль управления – это специальное программное обеспечение, устанавливаемое на АРМ администраторов безопасности, через которое производится подключение к Серверу и управление компонентами Аккорд-В. 2.0;

• Сервер – это программный модуль, который может быть установлен как на отдельный сервер, так и на АРМ администратора безопасности, и через который осуществляется централизованное управление всей системой защиты информации.

Взаимодействие между всеми компонентами Аккорд-В. 2.0 осуществляется при помощи RabbitMQ – брокера AMQP-сообщений. Выбор RabbitMQ обусловлен его преимуществами по сравнению с другими брокерами сообщений [11].

Сервер является центральным компонентом Аккорд-В. 2.0, который обрабатывает поступающие запросы от Консоли управления и напрямую задает настройки Агентов и Прокси-Сервера. Сервер подключается к центральной базе данных, в которую записывается и хранится вся информация о состоянии виртуальной инфраструктуры, а также все заданные настройки безопасности Агентов и Прокси-сервера.

На Сервере реализована система идентификации/аутентификации пользователей и поддержка нескольких ролей в системе: администратор безопасности и аудитор. Администратор безопасности имеет полный доступ в системе управления Аккорд-В. 2.0, а аудитор имеет права только на просмотр заданных настроек.

Администраторы безопасности через Консоль управления подключаются только к Серверу и через него осуществляют управление Аккорд-В. 2.0: устанавливают параметры доверенной загрузки виртуальных машин, задают правила разграничения доступа к функциям управления виртуальной инфраструктуры и т. д.

Агенты в ходе доверенной загрузки ВМ проверяют все ее параметры на соответствие эталонным значениям, заданным администратором безопасности. Важно, что эти модули работают независимо от Сервера: администратор безопасности настраивает через консоль управления Аккорд-В. 2.0 параметры работы Агента, а также выполняет установку ВМ на контроль. Агент позволяет контролировать разрешение на включение ВМ (то есть осуществляем контроль миграции), выполнять контроль целостности оборудования, BIOS, загрузочных записей дисков и файл-листов. Все параметры работы агента хранятся как локально на гипервизоре, так и в центральной базе данных. Благодаря этому после настройки Агенты работают автономно и не требует связи с Сервером. Такая децентрализация в принятии решений обеспечивает отказоустойчивость СЗИ за счет отсутствия единого центра принятия решений, который может стать единой точкой отказа.

СЗИ – это лишь инструмент, и оно позволяет строить систему защиты информационной системы, причем какой именно она должна быть и какие компоненты контролировать, каждая компания решает по-своему, в зависимости от модели угроз информационной системы. Аккорд-В. 2.0 позволяет гибко настраивать контроль целостности всех компонентов виртуальной машины. Это достигается через использование файл-листов, о которых мы говорили выше, а также через настройку списка контролируемого оборудования ВМ. Файл конфигурации ВМ может содержать сотни строк, описывающих ее оборудование. В зависимости от модели угроз и специфики обработки данных на этой ВМ список контролируемого оборудования может быть разным и Аккорд-В. 2.0 позволяет это учесть. Для каждого Агента может быть настроен список типов контролируемого оборудования: процессор, оперативная память, флоппи-диски, сетевые адаптеры и т. д. То есть если в Агента задан контроль сетевых адаптеров, то в ходе контроля оборудования ВМ будут проверяться значения строк файла конфигурации, отвечающих за сетевые адаптеры.

Для обеспечения контроля доступа администраторов ESXi к локальному управлению гипервизором (вопрос управления удаленным доступом рассматривается ниже) в состав Агента Аккорд-В. 2.0 входит подключаемый модуль идентификации и аутентификации пользователей.

Для разграничения доступа к функциям управления ВИ используется Прокси-сервер, который обрабатывает в соответствии с заданными правилами разграничения доступа все запросы, поступающие с рабочего места администратора ВИ на сервер управления vCenter (или на ESXi). Аккорд-В. 2.0 пропускает только разрешенные действия. Правила разграничения доступа на основе меток безопасности, задаваемых администратором безопасности через Консоль управления. Метка безопасности представляет собой совокупность значений двух параметров: иерархического уровня и неиерархических категорий. Стоит отметить, что

разделение объектов ВИ в соответствии с их метками безопасности и контроль перемещения этих объектов, при котором осуществляется сопоставление меток безопасности участвующих объектов, реализует сегментирование ВИ.

Все параметры работы Прокси-сервера, аналогично параметрам Агентов, хранятся как локально, так и в центральной базе данных. Это позволяет Прокси-серверу работать автономно, без связи с Сервером, что обеспечивает отказоустойчивость СЗИ.

Несмотря на то, что Аккорд-В. 2.0 позволяет разграничивать полномочия администраторов ВИ, после его установки в работе этих пользователей ничего не меняется: на рабочем месте не появляется дополнительных утилит, нет необходимости проходить аутентификацию в каких-либо дополнительных защитных сервисах, а для доступа к ВИ администратор может продолжать использовать привычный ему vSphere Client (HTML5) для работы. Изменяются только разве что настройки сети рабочего места пользователя – теперь трафик проходит через прокси-сервер.

Для обеспечения доверенной загрузки всех физических машин: АРМ администраторов, ESXi-сервера, vCenter в случае Windows Server может применяться модуль доверенной загрузки Аккорд-АМДЗ совместимый с Аккорд-В. 2.0.

Аккорд-В. 2.0 является наложенным средством защиты информации для платформы VMware vSphere и не ограничивает функциональные возможности и преимущества системы виртуализации.

Вывод. В ходе исследования были рассмотрены особенности защиты виртуальной инфраструктуры, построенной на платформе VMware vSphere, и сформулированы требования к средствам защиты информации виртуальных инфраструктур. В докладе на примере макета программы Аккорд-В. 2.0 было показано их выполнение. Конечно, были рассмотрены не все меры защиты, определенные в [3–5], выработка требований к средствам защиты, позволяющим реализовать указанные меры, будет выполнена в ходе дальнейшего исследования.

Список литературы

1. Маляревский А. Виртуализация как тренд 2020 [Электронный ресурс]. – Режим доступа : https://www.crn.ru/news/detail.php?ID=141879. – Дата доступа : 30.04.2021.

2. Защита систем виртуализации для VMware («Аккорд-В.» и «Сегмент-В.») [Электронный ресурс]// Официальный сайт ОКБ САПР. – Режим доступа : https://www.okbsapr.ru/products/virtsys/accord-v-and-segment-v/. – Дата обращения : 30.04.2021.

3. ГОСТ Р 56938-2016. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения [электронный ресурс]. – Режим доступа : http://docs.cntd.ru/document/1200135524. – Дата доступа : 30.04.2021.

4. Приказ № 17 ФСТЭК России от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

5. Приказ № 21 ФСТЭК России от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

6. Мозолина, Н. В. Использование атрибутной модели контроля доступа в задаче контроля целостности конфигурации / Н. В. Мозолина // Комплексная защита информации : мат-лы XXII науч.-практ. конф. Полоцк, 16-19 мая 2017 г. – Новополоцк : Полоц. гос. ун-т, 2017. – С. 87–90.

7. Защита систем виртуализации для KVM («Аккорд-KVM») [Электронный ресурс] // Официальный сайт ОКБ САПР. – Режим доступа : https://www.okbsapr.ru/products/virtsys/accord-kvm/. – Дата доступа : 30.04.2021.

8. Аккорд-АМДЗ [Электронный ресурс] // Официальный сайт ОКБ САПР. – Режим доступа : https://www.okbsapr.ru/products/accord/accord-amdz/. – Дата доступа : 30.04.2021.

9. СПО Аккорд-Win64 [Электронный ресурс] // Официальный сайт ОКБ САПР. – Режим доступа : https://www.okbsapr.ru/products/accord/spo-accord-win64-k/. – Дата доступа : 30.04.2021.

10. Мозолина, Н. В. Защита виртуализации «в эпоху бурного развития» / Н. В. Мозолина // Information Security/Информационная безопасность. – 2019. – № 1. – С. 29.

11. Чадов, А. Ю. Сравнительный анализ AMQP брокеров сообщений для использования в качестве элемента децентрализованной системы разграничения доступа / А. Ю. Чадов, К. Э. Михальченко // Комплексная защита информации : мат-лы XXIV науч.-практ. конф. Витебск. 21–23 мая 2019 г. – Витебск : УО ВГТУ, 2019. – С. 261–267.

УДК 004.58

АКТУАЛЬНОСТЬ НОРМАТИВНО-ПРАВОВЫХ АКТОВ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ ДЛЯ ЛОКАЛЬНЫХ СЕТЕЙ ГОСУДАРСТВЕННЫХ ПРЕДПРИЯТИЙ

А.М. МАЖЕЙКО, Е.С. БЕЛОУСОВА
Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Введение. В Республике Беларусь с 2008 года государственным органом, осуществляющим регулирование деятельности по обеспечению защиты информации, является Оперативно-аналитический центр при Президенте Республики Беларусь (ОАЦ). Основными задачами ОАЦ является разработка и внедрение в практику нормативно-правовых актов, обязательных к применению на критически важных объектах информатизации и информационных системах [1].

В настоящее время с 20.02.2020 года на территории Республики Беларусь действует приказ ОАЦ № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449», который заменяет пакет ранее изданных документов [2].

Требования данных документов необходимо использовать в качестве основы для разработки внутренних локальных нормативно-правовых актов по технической защите информации и/или политики информационной безопасности предприятия.

Результаты, представленные в данной работе, получены на основе практического опыта внедрения нормативно-правовых актов, изучения вопроса эффективности их внедрения и необходимости принятия дополнительных мер по повышению безопасности в локальных сетях государственных предприятий.

1. Разработка локальных нормативно-правовых актов государственного предприятия по информационной безопасности. Разработка актов состояла из нескольких этапов:

1. Составление перечня информационных ресурсов предприятия, подлежащих защите.

2. Определение списка вопросов в нормативно-правовой базе, которые описывают требования к защите ресурсов предприятия.

3. Подготовка и издание локальных нормативно-правовых актов по защите информации предприятия.

Ввиду наличия инцидентов информационной безопасности после вступления в силу изданных актов было принято решение о проведении контроля за их исполнением, а именно аудита информационной безопасности предприятия.

2. Контроль за исполнением локальных нормативно-правовых актов. Для контроля эффективности внедрения политики безопасности на основе принятых документов была разработана методика аудита информационной безопасности, в которой было уделено внимание следующим блокам вопросов:

1. Исключение подключения личных мобильных устройств к ПЭВМ.

2. Запрет на установку программного обеспечения лицами, не уполномоченными на данное действие.

3. Запрет использования ПЭВМ для целей, не связанных с деятельностью работника (например, хранение и использование игр, фильмов, музыки);

4. Исключение нарушений правил пользования сетью Интернет.

Аудит информационной безопасности по разработанной методике был проведен в 7 подразделениях государственного предприятия. Суммарное количество проверенных ПЭВМ во всех аудитах составило 398 единиц, что в среднем составляет более 56 ПЭВМ на каждый аудит. По материалам аудитов была собрана статистика нарушений по исполнению требований политики информационной безопасности.

3. Результаты аудитов информационной безопасности. По результатам аудитов были собраны статистические данные по нарушениям политики информационной безопасности (табл. 1).

Таблица 1

Доли ПЭВМ, имеющих нарушения в каждом аудите

Блок вопросов	Аудит						
	1	2	3	4	5	6	7
1	53 %	3 %	9 %	4 %	24 %	6 %	8 %
2	7 %	5 %	4 %	0 %	28 %	21 %	5 %
3	12 %	0 %	2 %	4 %	8 %	2 %	8 %
4	4 %	0 %	20 %	2 %	0 %	4 %	3 %

По результатам внедрения нормативно-правовых актов и последующих аудитов отмечается снижение процентного количества нарушений.

Заключение

1. Практическое внедрений нормативно-правовых актов по технической защите информации для локальных сетей государственных предприятий имеет несомненную актуальность.

2. Нормативно-правовая база позволяет разработать политику информационной безопасности для государственного предприятия без привлечения сторонних организаций и существенно сократить расходы государственного бюджета на выполнение работ по защите информации.

3. Разработка документации может выполняться поэтапно, а также в объеме, определенном руководителем и работниками предприятия.

4. Внедрение организационных мер по защите информации является обязательным этапом для создания комплексной системы защиты информации предприятия.

Необходимо отметить, что основные сложности внедрения организационных мер по защите информации заключаются в необходимости контроля за их исполнением. В определенной степени данную функцию выполняют аудиты информационной безопасности предприятия. Также дополнительно требуются и технические средства защиты ввиду наличия сознательных нарушений нормативно-правовых актов по технической защите информации.

Список литературы

1. Информация об ОАЦ // Оперативно-аналитический центр при Президенте Республики Беларусь [Электронный ресурс] – Режим доступа : https://oac.gov.by/info. – Дата доступа : 23.04.2021.

2. О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 [Электронный ресурс] : Приказ Оперативно-аналитического центра при Президенте Республики Беларусь, 20 февраля 2020 г., № 66 // Оперативно-аналитический центр при Президенте Республики Беларусь. – Режим доступа : https://oac.gov.by/public/content/files/files/law/prikaz-oac/2020%20-%2066.pdf. – Дата доступа : 23.04.2021.

УДК 004.942

АППАРАТНЫЙ РКБ НА СЛУЖБЕ СДЗ УРОВНЯ BIOS

А.Д. ХМЕЛЬКОВ
ФРКТ МФТИ, г. Москва, Российская Федерация

Доверенная загрузка (т. е. загрузка операционной системы только с заранее установленных носителей после успешного завершения процедур контроля целостности технических и программных средств вычислительной техники (далее – СВТ) с использованием метода пошагового контроля целостности и аппаратной идентификации/аутентификации [1]) – один из важнейших этапов обеспечения СВТ от несанкционированного доступа (далее – НСД). Наличие угрозы НСД (а точнее недоверенной загрузки ОС и, как следствие, возможное нарушение конфиденциальности/целостности/доступности информации на защищаемом СВТ) и наличие недостатков у существующих решений по обеспечению доверенной загрузки (о них далее) делают актуальной задачу разработки более совершенного решения для обеспечения доверенной загрузки.

Цель данной работы – предложить программно-аппаратное решение, позволяющее осуществить доверенную загрузку ОС и лишенное недостатков, имеющихся при использовании программных и аппаратных средств защиты по отдельности. Для этого необходимо провести обзор существующих типов СДЗ, выявить их недостатки и на основании проведенного анализа предложить новое решение. Решения, предложенные для реализации механизма доверенной загрузки, можно разделить на три типа в соответствии с классификацией ФСТЭК: средства доверенной загрузки (далее – СДЗ) уровня базовой системы ввода-вывода (уровня BIOS), СДЗ уровня платы расширения и СДЗ уровня загрузочной записи [2]. СДЗ уровня загрузочной записи в данной работе рассматриваться не будут, т.к. могут быть сертифицированы ФСТЭК лишь по 5 и 6 классу защиты, что для настоящей статьи неактуально.

СДЗ уровня BIOS встраиваются непосредственно в BIOS защищаемого СВТ. Точнее, внутрь BIOS обязательно встраивается модуль, осуществляющий передачу управления специальному программному обеспечению (далее – СПО) СДЗ и реализующий базовые проверки безопасности, такие как идентификация/аутентификация и контроль целостности. База данных, журнал и функциональное программное обеспечение (далее – ФПО), входящее в состав СДЗ, может находиться как внутри BIOS, так и вне его, например, на жестком диске защищаемого СВТ. Недостаток данного решения в том, что оно не обеспечивает защиту самого BIOS. Вредоносный код может быть встроен не только в операционную систему, но и непосредственно в BIOS, что подтверждается различными исследованиями [3, 4]. Также без аппаратной части невозможна реализация физического датчика случайных чисел (далее – ДСЧ) и сторожевого таймера.

Штатные средства защиты BIOS существуют, однако они платформозависимы и производятся теми же организациями, что и сами BIOS, т. е. в большинстве случаев иностранными организациями. Следовательно, доверять таким средствам можно не больше, чем самому BIOS.

СДЗ уровня платы расширения – это аппаратно-программный модуль доверенной загрузки (далее – АПМДЗ). Он представляет собой некую «железку», которая вставляется в один из слотов СВТ через такие интерфейсы как PCI/PCI-express/mini PCI-express, M2, USB и другие [5–7]. Вся начинка СДЗ находится в защищенной памяти этой платы, что существенно затрудняет модификацию/удаление ФПО или базы данных злоумышленником. У такого решения также имеются недостатки. Во-первых, дороговизна самого устройства. Во-вторых, необходимо наличие свободного слота для устройства. В-третьих, внешнее устройство стартует позже, чем встроенный в BIOS модуль, что делает работу BIOS менее безопасной.

В таблице 1 наглядно показано сравнение преимуществ и недостатков СДЗ уровня BIOS и СДЗ уровня платы расширения.

Рассмотрев недостатки существующих решений, можно предъявить к разрабатываемому СДЗ следующие дополнительные требования:

– как можно более ранний старт,

– возможность проверки целостности BIOS,
– возможность аппаратной реализации ДСЧ и сторожевого таймера,
– как можно более низкая стоимость реализации.

Таблица 1

Сравнение СДЗ уровня BIOS и СДЗ уровня платы расширения

Параметр	СДЗ уровня BIOS	СДЗ уровня платы расширения
Ранний старт	+	-
Контроль целостности BIOS	-	+
Защищенная память	-	+
Сторожевой таймер	-	+
Аппаратный ДСЧ	-	+
Низкая стоимость	+	-

Выполнения требований можно добиться, если два типа СДЗ (уровня BIOS и уровня платы расширения) соединить в одном, создав некое гибридное неатоматрное [8] решение. И действительно, то, что является преимуществом одного типа СДЗ, является одновременно недостатком другого и наоборот. Объединение двух типов СДЗ в один в такой ситуации кажется логичным. СДЗ уровня BIOS может представлять собой DXE-драйвер, осуществляющий перехват управления и базовые проверки. Все остальные компоненты СДЗ будут располагаться в аппаратном модуле. По сравнению с обычным СДЗ уровня BIOS данное решение позволит использовать защищенную память: база данных, журнал, криптографические данные будут защищены от модификации. Также плюсом будет возможность использования аппаратного ДСЧ, который, в отличии от программных аналогов, позволяет получать истинно случайные числа. Аппаратная составляющая также необходима для реализации сторожевого таймера. Данный механизм перезагрузит СВТ, если в течение определенного времени СДЗ не получит управление. Плюсом по сравнению с чисто аппаратной реализацией СДЗ будет стоимость: необходимое для реализации «железо» значительно дешевле, чем АПМДЗ, ведь от аппаратной части будет требоваться только наличие памяти, ДСЧ и сторожевого таймера, а все вычисления будут производиться ресурсами СВТ. Возможность реализации аппаратной части в форм-факторе USB делает устройство практически универсальным. Дополнительным преимуществом будет более ранний старт. Внешние устройства при запуске UEFI BIOS стартуют на этапе DXE, в то время как встроенный модуль может запускаться на этапе PEI, который, согласно стандарту работы UEFI BIOS, происходит раньше [9].

В данной работе был проведен обзор преимуществ и недостатков различных типов СДЗ, а затем предложено и описано решение, объединяющее в себе два типа СДЗ, которое не обладает рядом характерных для каждого типа в отдельности недостатков. Следующими шагами в работе видится непосредственная разработка устройства и его последующие испытания.

Список литературы

1. Конявский, В. А. Управление защитой информации на базе СЗИ НСД «Аккорд» / В. А. Конявский. – М. : «Радио и связь», 1999. – 325 с.

2. Информационное письмо ФСТЭК России от 6 февраля 2014 г. №240/24/405.

3. Счастный, Д. Ю. БИОС под аппаратным надзором / Д. Ю. Счастный // Комплексная защита информации : мат-лы XXIV науч.-практ. конф. Витебск. 21–23 мая 2019 г. – Витебск : УО ВГТУ, 2019. – С. 212–215.

4. Голованов С., Русаков В. Атаки до загрузки системы [Электронный ресурс] / С. Голованов, В. Русаков. – Режим доступа : https://securelist.ru/ataki-do-zagruzki-sistemy/20151/. – Дата доступа : 11.05.2021.

5. Аккорд-АМДЗ [Электронный ресурс] // Официальный сайт компании «ОКБ САПР». – Режим доступа : https://www.okbsapr.ru/products/accord/accord-amdz/. – Дата доступа : 11.05.2021.

6. СДЗ НСД «ИНАФ» [Электронный ресурс] // Официальный сайт компании «ОКБ САПР». – Режим доступа : https://www.okbsapr.ru/products/accord/szi-nsd-inaf/. – Дата доступа : 11.05.2021.

7. Соболь. Модельный ряд [Электронный ресурс] // Официальный сайт компании «Код безопасности». – Режим доступа : https://www.securitycode.ru/products/pak_sobol/?tab=models. – Дата доступа : 11.05.2021.

8. Алтухов, А. А. Неатомарный взгляд на РКБ, как на композицию перехвата управления и контроля целостности / А. А. Алтухов // Комплексная защита информации : мат-лы XX науч.-практ. конф. Минск, 19–21 мая 2015 г. – Минск : РИВШ, 2015. – С. 53–55.

9. Черчесов, А. Э. Фазы загрузки UEFI и способы контроля исполняемых образов / А. Э. Черчесов // Вопросы защиты информации. – 2018. – № 2 (121). – С. 51–53.

УДК 621.391, 004.056.5

АРХИТЕКТУРА ВОЛОКОННО-ОПТИЧЕСКОГО КАНАЛА ПЕРЕДАЧИ СИГНАЛА ДЛЯ МАСКИРОВАНИЯ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Е.Р. АДАМОВСКИЙ, В.К. ЖЕЛЕЗНЯК, Д.Г. САПЕЖКО
Полоцкий государственный университет,
г. Новополоцк, Республика Беларусь

Введение. Активная защита КУИ путем обеспечения электромагнитного зашумления распределенного в пространстве объекта информатизации (например, ряд выделенных помещений) может быть выполнена с использованием множества локальных генераторов шума (ГШ). Недостатком способа является сложность централизованного управления и содержания такой системы по причине необходимости обслуживания большого количества технически сложных устройств.

Предлагается способ с использованием одного ГШ, маскирующий сигнал которого вместе с контрольной суммой передается по внутренней линии связи (локальной сети), разветвляется и передается в каждое помещение, где может быть усилен и излучен в канал утечки информации (КУИ). Преимуществами решения являются: использование меньшего количества обслуживаемой аппаратуры, возможность реализации центрального удаленного управления системой с высокой степенью автоматизации и автономности.

При передаче сигнала с помощью «витой пары» по длинной линии связи (свыше 100 метров) проявляются недостатки медного кабеля: рабочая емкость (30-50 нФ/км [1]) и индуктивность (250-400 мГн/км [2]); подверженность влиянию внешних факторов (электромагнитные наводки, перепады температуры, высокая влажность и т. д.); большая величина затухания сигнала α (выражаемая в дБ/км), пропорциональная его частоте. В качестве примера, в табл. 1 приведена взаимосвязь величины затухания сигнала от частоты для радиочастотного кабеля РК 75-4-12, производимого на предприятии «Беларускабель» [3], рассчитанная с помощью специализированного онлайн-инструмента [4].

Таблица 1

Зависимость $\alpha(f)$ для радиочастотного кабеля РК 75-4-12

Частота, кГц	0.1	0.5	1	5	10	50	100	500
Затухание, дБ/км	0.11	0.26	0.36	0.81	1.15	2.56	3.63	8.12

Из таблицы 1 следует, что высокочастотные колебания сигнала за счет больших погонных потерь при прохождении через медный кабель будут в значительной мере подавлены, следовательно, выходной сигнал окажется искаженным.

Недостатки предложенной системы защиты объекта информатизации могут быть устранены за счет использования в качестве линии связи сигнала волоконно-оптического кабеля (ВОЛС), который слабо подвержен внешним воздействиям, практически не искажает сигнал, более легкий по сравнению с медным кабелем, а также имеет малое значение затухания α (для лучших промышленных образцов до 0.18-0.19 дБ/км [5, 6]).

Передача данных через ВОЛС может осуществляться аналоговыми и цифровыми сигналами, для которых исходный электрический сигнал в первую очередь должен быть подвергнут процедурам дискретизации и квантования с помощью аналого-цифрового преобразователя (АЦП), а затем – передан в оптическую линию связи через модулятор, преобразующий электрический сигнал в световой поток. На приемной стороне над оптическим сигналом требуется произвести демодуляцию и обработать цифро-аналоговым преобразователем (ЦАП).

Преимущество схемы с передачей аналогового сигнала заключается в более простой реализации схемы без устройств АЦП и ЦАП, но при этом результирующий сигнал может быть искажен и ослаблен. Использование цифрового сигнала обеспечивает полное восстановление формы исходных данных за счет его способности к регенерации. Однако, верхняя

частота такого сигнала, согласно теореме Котельникова, на практике ограничена половиной частоты дискретизации АЦП и ЦАП.

Как правило, для передачи информации в стандартном оптическом волокне со ступенчатым профилем используются три окна прозрачности на длинах волн 850 нм, 1310 нм и 1550 нм (соответствующие значения α 2-2.5 дБ/км, 0.5 дБ/км и 0.22 дБ/км). При этом, чем меньше длина волны, тем меньшие дополнительные потери испытывает волокно при макро-изгибах [7], что может быть значимым фактором при прокладке ВОЛС внутри коммуникаций объекта информатизации, характеризующихся резкими поворотами в ограниченном пространстве.

Теоретическая модель. Реализация системы защиты объекта информатизации основана на использовании ВОЛС в качестве канала передачи маскирующего сигнала в цифровом виде. Может передаваться последовательность, предназначенная для защиты любого сигнала, в том числе аудио и видеоинформации. В работах [8, 9] обосновано использование хаотической импульсной последовательности (ХИП) и ее адаптивного варианта в качестве маскирующего сигнала для голосовых записей и видеопоследовательностей. Схема, реализующая передачу маскирующего сигнала через оптический канал связи, показана на рис. 1.

Генератор шума ХИП (1) формирует электрический сигнал $s(t)$ (2), который подается на вход АЦП (3.1), где на его основе формируется двоичная последовательность символов h (3.2):

$$h = \left[(h_{11}, h_{12}...h_{1M})(h_{21}, h_{22}...h_{1M})...(h_{L1}, h_{L2}...h_{LM})\right] \quad (1)$$

где M – разрядность АЦП (бит), количество его уровней квантования, следовательно, длина цифрового кода на одно измерение;

L – число отсчетов, которое зависит от длительности сигнала и частоты дискретизации АЦП $f_{АЦП}$.

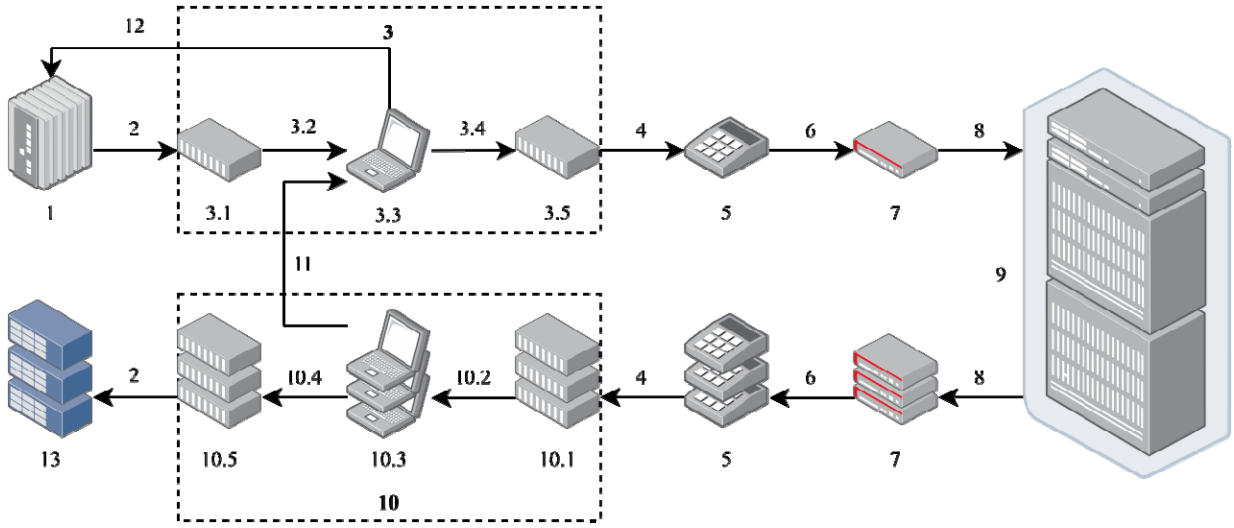


Рис. 1. Схема системы передачи маскирующего сигнала с контрольной суммой при использовании ВОЛС на базе локальной сети объекта информатизации

Цифровой сигнал h поступает для обработки в оперативную память средства вычислительной техники (3.3) (СВТ), в качестве которого выступает персональный компьютер (ПК) в виде стационарного устройства или переносного ноутбука, снабженного соответствующим программным обеспечением (ПО). В дальнейшем последовательность отсчетов h может быть дополнена сигналом контрольной суммы с целью мониторинга качества передачи и гарантии его безопасности на приемной стороне, а также сохранена в долговременную память устройства при необходимости, как h' (3.4). После соответствующей обработки, с помощью ЦАП (3.5), последовательность h' восстанавливается до аналогового сигнала с контрольной суммой $s'(t)$ (4).

Сигнал $s'(t)$ подается на телефонный аппарат (5) через разъем *RJ-11*, соединяющий его с голосовой трубкой. В свою очередь, устройство подключается аналогичным способом к модему (7), служащему в качестве преобразователя телефонного сигнала (6) в цифровую форму и модулятора оптического/электрического излучения. Сигнал модема (8) поступает в локальную сеть и перенаправляется управляющими маршрутизирующими устройствами (9) на заданные адреса, определяемые при наборе номера телефона [10].

Прием реализован способом, обратным способу передачи данных. Оптический модем принимает сигнал, преобразует и передает его на телефон, где происходит восстановление исходной формы $s'(t)$. Данный сигнал подается на контрольный ПК (10), где осуществляется проверка контрольной суммы сигнала и принимается решение о продолжении или прерывании сеанса передачи данных при снижении качества приема ниже порогового значения. Контрольные сигналы (11), предназначенные для управляющего ПК (3.3), могут быть переданы любым способом, на основе которых происходит управление (12) ГШ. Результирующий сигнал дополнительно усиливается и излучается в КУИ (13).

Система связанных устройств АЦП – ПК – ЦАП (3, 10, рис. 1) для обработки маскирующего аудио-сигнала может быть представлена в виде единого компактного блока способом, указанным на рис. 2. В таком случае верхняя частота сигнала ограничена частотой дискретизации АЦП используемой звуковой карты. Характерные параметры современных устройств: $f_{АЦП}$ = 192 кГц, разрядность 24-32 бит.

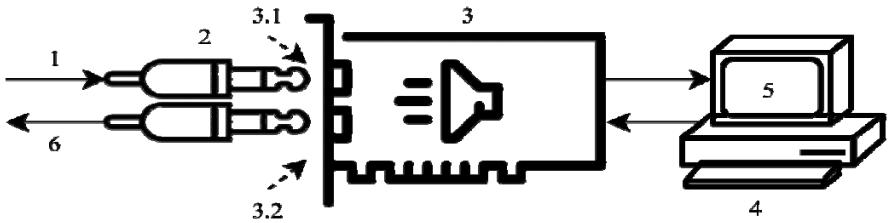


Рис. 2. Реализация обработки маскирующего аудио-сигнала с помощью звуковой карты ПК:
1 – источник сигнала; *2* – разъем *mini-jack* 3.5 мм; *3* – звуковая карта;
3.1 – АЦП; *3.2* – ЦАП; *4* – ПК; *5* – ПО; *6* – приемник сигнала

Схема может быть реализована при полном или частичном отсутствии оптоволоконной инфраструктуры на объекте информатизации, но в таком случае ее эффективность будет снижена по причине того, что использование медных кабелей типа «витая пара» не обеспечивает высокую скорость передачи данных в сравнении с оптоволокном, а также имеет меньшую защищенность.

Моделирование. Программная обработка сигнала реализована с помощью пакета *MatLab R2021a*. Для проверки работоспособности предложенной модели в качестве маскирующего сигнала использована треугольная последовательность с частотой 60 Гц. Прием сигнала смоделирован путем добавления шума небольшого уровня и его случайного смещения. Подробное описание модели включает пункты:

1. Подготовка данных из ГШ выполняется пакетным способом двумя параллельно работающими процессами. В первом процессе входной сигнал разбивается на небольшие отрезки длительностью до нескольких секунд. Для каждого фрагмента вычисляется среднее значение – контрольная сумма, представление которой вставляется в начало отрезка с длительностью, равной 5-10% от количества его отчетов. Пакеты генерируются заданное количество раз, объединяются и сохраняются для дальнейшей передачи. После этого цикл повторяется.

2. Второй процесс отслеживает появление новых пакетов и воспроизводит их в канал передачи. При появлении в указанном каталоге очередного файла, происходит его считывание и проигрывание с помощью звуковой карты.

3. Прием сигнала осуществляется в реальном времени процессом, в задачи которого входит определение границы пакетов, выделение и удаление из них сигнала контрольной суммы, принятие решения о продолжении или прерывании передачи на основе сравнения разницы между контрольной суммой и сигналом, а также пороговой величиной.

В реальности обеспечение синхронизации управляющего и приемного ПК может быть затруднено, поэтому принимается, что сигнал поступает в приемник непрерывным потоком,

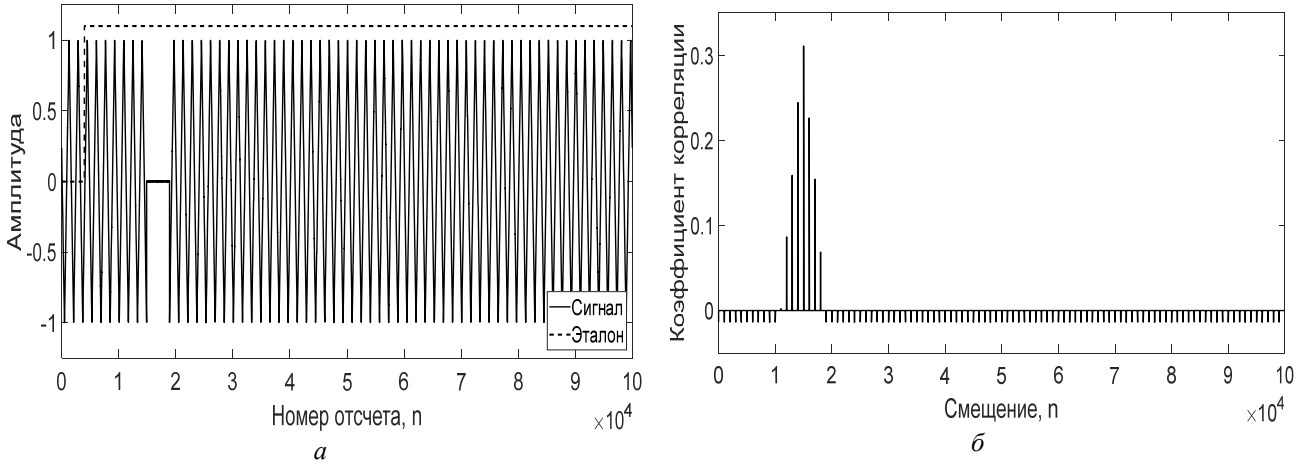
для которого требуется автоматизированное определение границы блоков. Пример реализации данного функционала, которая основана на вычислении коэффициента корреляции фрагмента сигнала с эталоном особой формы, приведена в листинге 1. Результаты работы алгоритма показаны на рис. 3.

Листинг 1

Пример реализации обнаружения границ блока и выделения из него контрольной суммы

```
%% СИГНАЛ N, КОНТРОЛЬНАЯ СУММА M
template = [zeros(1, M) ones(1, N – M)];        % эталон
part = signal(((j-1)*N)+1*(j-1)*N)+N);          % чтение блока данных
part = part / max(part);                        % нормировка сигнала
for i = 1:N/100:N                               % цикл по сигналу с шагом 1%
    template_ = circshift(template, i);         % циклическое смещение эталона
    corr = corrcoef(template_, abs(part));      % вычисление коэфф. корреляции
    mass_corr(i) = corr(1, 2);                  % запись в массив результата
end
[max_val, max_pos] = max(mass_corr);            % получение валидного смещения
part = circshift(part, -max_pos);               % смещение фрагмента сигнала
control = abs(mean(part(1:M)));                 % чтение контрольной суммы
reals = abs(mean(part(M + 1:end)));             % чтение данных
dif = abs(control – reals);                     % сравнение данных и суммы
```

На рис. 3 продемонстрирована возможность обнаружения местоположения фрагмента контрольной суммы в случайно сдвинутом сигнале, следовательно, потокового приема сигнала и его обработки в реальном времени.



а *б*

Рис. 3. Автоматизированное выравнивание блоков сигнала:
а – блок информации и эталон; *б* – корреляционная функция смещения

Заключение. Результатом исследования является подтверждение возможности реализации архитектуры ВОЛС для передачи сигнала с целью распределенного маскирования объекта информатизации, а также других информационных сигналов для сигнализации, мониторинга и т. д.

Предложенная модель использует в качестве среды распространения оптические линии связи, предназначенные для сетевых локальных соединений Ethernet, следовательно, задействуется соответствующее оборудование и протоколы передачи цифровых данных, которые в первую очередь определяют качество и скорость соединения узлов.

Дальнейшее развитие модели включает в себя разработку программно-аппаратного комплекса, реализующего передачу исходного маскирующего сигнала с помощью ВОЛС без использования локальных Ethernet-сетей за счет применения специализированных оптико-электрических преобразователей и соответствующего программного комплекса, реализующего собственные протоколы передачи.

Список литературы

1. Абрамов, К. К. Расчет электрических емкостей многожильного кабеля с комбинированной изоляцией / К. К. Абрамов // Кабели и провода. – 2009. – № 3 (316). – С. 3–9.

2. Радкевич, В. Н. Определение индуктивных сопротивлений одножильных кабелей с изоляцией из сшитого полиэтилена напряжением до 1 кВ / В. Н. Радкевич, В. В. Сталович, Д. С. Алехнович // Энергетика. изв. высш. учеб. заведений и энерг. объединений СНГ. – 2018. – Т. 61, № 4. – С. 321–333.

3. Беларускабель: Радиочастотные кабели [Электронный ресурс] / РК 754-12. – Режим доступа : https://belaruskabel.by/catalog/radiochastotnye_kabeli/rk_754_12/. – Дата доступа : 20.04.2021.

4. Расчет затухания в коаксиальном кабеле [Электронный ресурс]. – Режим доступа : https://www.ivtechno.ru/raschet_5. – Дата доступа : 20.04.2021.

5. Листвин, А. В. Оптические волокна для линий связи: учеб. пособие / А. В. Листвин, В. Н. Листвин, Д. В. Швырков. – М. : ЛЕСАРарт, 2003. – 106 с.

6. Шарварко, В. Г. Волоконно-оптические линии связи : учеб. пособие / В. Г. Шарварко. – Таганрог : Изд-во ТРТУ, 2006. – 170 с.

7. Косари, А. Г. Обнаружение каналов утечки информации в оптоволоконных линиях связи на основе маломощных оптических воздействий : автореф. … канд. техн. наук: 05.13.19 Методы и системы защиты информации, информационная безопасность / А. Г. Косари. – Минск, 2016. – 24 с.

8. Бураченок, И. Б. Обнаружение измерительных сигналов в маскирующих шумах высокого уровня / И. Б. Бураченок, В. К. Железняк, А. Г. Филиппович // Вест. Полоц. гос. ун-та. Сер. С, Фундам. науки. – 2018. – № 4. – С. 2–9.

9. Железняк, В. К. Метод адаптивного маскирования видеокадра маскируемым сигналом / В. К. Железняк, Е. Р. Адамовский // Вест. Полоц. гос. ун-та. Сер. С, Фундам. науки. – 2019. – № 4. – С. 2–6.

10. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 4-е изд. – СПб. : Питер, 2010. – 944 с.

УДК 004.056

НЕЙРО-СЕТЕВАЯ ОПТИМИЗАЦИЯ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПРИ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЯХ

Л.О. ГОЛОВИН, Е.А. МАКСИМОВА
МИРЭА – Российский технологический университет (РТУ МИРЭА),
г. Москва, Российская Федерация

Введение. Современные информационные инфраструктуры способны обрабатывать большое количество данных. При этом, для них одной из приоритетных задач в области информационной безопасности (ИБ) является обеспечение надежной и устойчивой доступности к данным [1]. С введением 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [2] данный вопрос актуализировался и для объектов критической информационной инфраструктуры (КИИ).

При решении обозначенного вопроса, в том числе исследуются вопросы, связанные с несанкционированным использованием трафика через внешнюю сеть Интернет [3]. Как результат – нарушение доступности к данным на уровне субъекта КИИ (СКИИ). Так как в процессе расследования сложившегося инцидента ИБ «пораженный» объект будет «изолирован», а СКИИ при этом должен функционировать, то предлагается перераспределение в СКИИ поступающих на «изолированный» объект запросов. Для решения обозначенной задачи предлагается использование искусственных нейронных сетей.

1. Обоснование метода исследования. В качестве используемых сегодня подходов при работе с защитой данных в СКИИ предлагается, например, подход на основе анализа пространства параметров процессов в информационной инфраструктуре по установленным правилам и выявлению параметров, которые характеризуют действие атаки. В данном случае, разработанная модель позволяет решать задачу путем нахождения полного множества безопасных состояний информационной инфраструктуры. При этом констатируется, что сложность решения таких задач заключается в описании объекта моделирования – КИИ [4].

В работе [5] в ходе проведения исследования предложен метод обучения «без учителя» импульсной искусственной нейронной сети. Выходной слой отдает сигналы-импульсы и преобразуются в правила фильтрации. Такая нейронная сеть позволяет защищать объекты КИИ от DDoS-атак.

Моделирование искусственных нейронных сетей для защиты СКИИ при деструктивных воздействиях, является актуальным, но практически не используемым на настоящий момент [6, 7]. В качестве преимуществ искусственных нейронных сетей при этом можно обозначить быстродействие, способность к обучению, отказоустойчивость и устойчивость к шумам во входных данных.

2. Описание СКИИ как системы. Согласно [2] КИИ – это совокупность объектов критической информационной инфраструктуры. Объекты КИИ в структуре субъекта КИИ (СКИИ) находятся во взаимодействии. С целью повышения эффективности модели защиты данных на уровне СКИИ нами предлагается выполнить линейную структуризацию СКИИ: выделение подсистем взаимодействующих объектов КИИ. При этом, возможны ситуации межобъектного взаимодействия на уровне одного субъекта (рис. 1) либо на межсубъектном уровне (рис. 2).

Предположим, что существует СКИИ с конечным набором топологическираспределенных объектов КИИ. Структурные элементы СКИИ как системы – подсистемы взаимодействующих объектов. Соответствующие подсистемы обслуживают запросы пользователей (рис. 3). *A, B, C* – подсистемы взаимодействующих объектов СКИИ. В процессе функционирования СКИИ выполняется запрос пользователя, например, к объекту *A.3*, как это показано на рисунке.

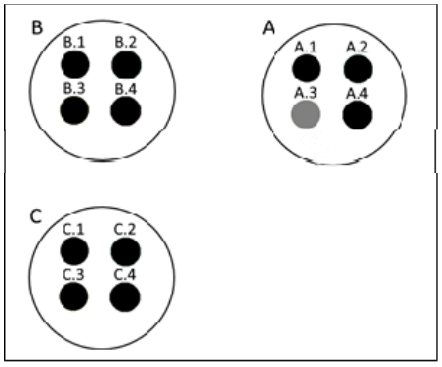


Рис. 1. Модель межобъектного взаимодействия на уровне одного субъекта

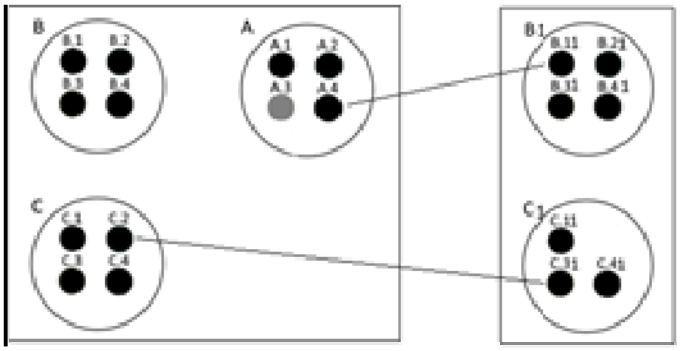


Рис. 2. Модель межобъектного взаимодействия на межсубъектном уровне

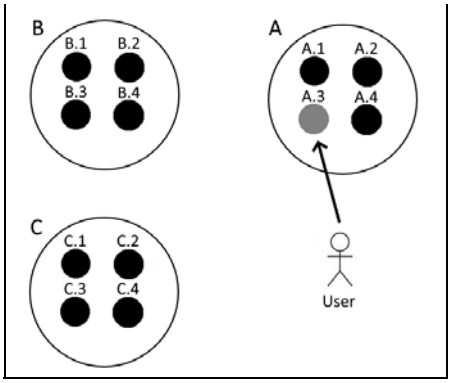


Рис. 3. Пример структурной схемы субъекта критической информационной структуры

4. Модель нейро-сетевой оптимизации критической информационной инфраструктуры при деструктивных воздействиях. При совершении деструктивного воздействия на объект *A.3* данный объект становится недоступным в следствии процедурной изоляции после обнаружения инцидента. Запрос пользователя этим объектом уже обработаться не может. Следовательно, будем перераспределять запрос пользователя на объект КИИ с аналогичным функционалом (рис. 4).

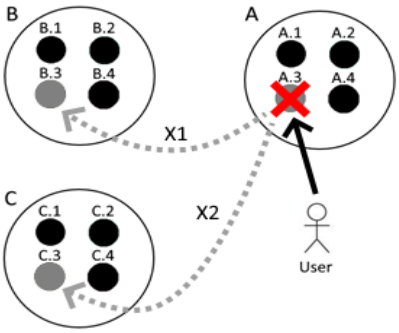


Рис. 4. Модель перераспределения запросов пользователя после обнаружения деструктивного воздействия на объект КИИ

Так как в рассматриваемой ситуации возможно перераспределение запросов пользователей в вариантах либо «один к одному», либо «один ко многим» в зависимости от количества запросов и количества объектов КИИ, которые данный запрос (запросы) могут обработать, то задача выходит на уровень оптимизационной задачи.

В ходе изучения доступных наборов данных, к сожалению, на текущий момент, нет абстрактных моделей СКИИ, которые подходят для решения данной задачи. Таким образом, для построения модели нейро-сетевой оптимизации КИИ при деструктивных воздействиях сформированы три набора случайных гауссовых двумерных векторов:

$$\left\{\vec{x}_i\right\}^{(1)}, \left\{\vec{x}_i\right\}^{(2)}, \left\{\vec{x}_i\right\}^{(3)}$$

с параметрами:

$$\left\{\vec{\mu}_1, \Sigma_1\right\}^{(1)}, \left\{\vec{\mu}_2, \Sigma_2\right\}^{(2)}, \left\{\vec{\mu}_3, \Sigma_3\right\}^{(3)},$$

где $\left\{\vec{x}_i\right\}^{(j)}$ – гауссовый двумерный вектор;

$\vec{\mu}_j$ – математическое ожидание позиции гауссового двумерного вектора;

Σ_2 – корреляционная матрица.

Архитектура модели нейро-сетевой оптимизации КИИ при деструктивных воздействиях (рис. 5) представлена набором модулей из 4 полносвязных слоев:

1. Первый полносвязный слой имеет 25 нейронов и линейную функцию активации;
2. Второй полносвязный слой имеет 100 нейронов и сигмоидную функцию активации;
3. Третий полносвязный слой имеет 15 нейронов и функцию активации ReLU;
4. Четвертый выходной полносвязный слой имеет 2 нейрона на выходе и функцию активации Softmax.

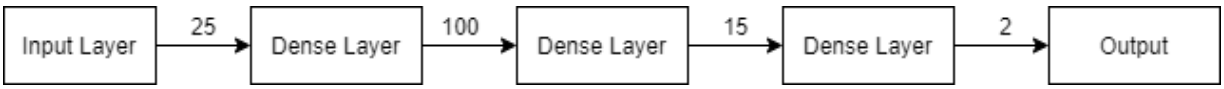


Рис. 5. Архитектура модели нейро-сетевой оптимизации КИИ при деструктивных воздействиях

Представленная модель апробирована в серии экспериментов, в ходе которых выполнялось обучение нейронной сети с низким значением ошибки 0.02 и точностью в 0.98. Результаты тестов показали, что процент ошибки на тестовых данных так же является 2%.

Заключение. Представленная модель нейро-сетевой оптимизации КИИ при деструктивных воздействиях позволила решить задачу оптимизации КИИ путем перераспределения запросов пользователя при деструктивных воздействиях на ее объекты.

Предложенная модель нейро-сетевой оптимизации КИИ при деструктивных воздействиях может применяться для оптимизации КИИ на всех уровнях инфраструктурной иерархии.

Благодарности. Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ, проект № 3/2020).

Список литературы

1. Максимова, Е. А. Оценка информационной безопасности субъекта критической информационной инфраструктуры при деструктивных воздействиях / Е. А. Максимова. – Волгоград : Изд-во ВолГУ, 2020. – 95 с.

2. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26.07.2017 № 187-ФЗ [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_220885/. – Дата доступа : 30.03.2021.

3. Максимова, Е. А. Исследование алгоритмов безопасной передачи данных между объектами критической информационной инфраструктуры / Е. А. Максимова // Сб. докладов XXIII пленума ФУМО ВО ИБ и Всероссийской научной конференции «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (ИНФОБЕЗОПАСНОСТЬ-2019). – 2019. – С. 157–163.

4. Шабуров, А. С. О разработке модели обнаружения компьютерных атак на объекты критической информационной инфраструктуры / А. С. Шабуров // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2018. – №. 26.

5. Пальчевский, Е. В. Разработка импульсной нейронной сети с возможностью скоростного обучения для нейтрализации DDoS-атак / Е. В. Пальчевский, О. И. Христодуло // Программные продукты и системы. – 2019. – Т. 32, № 4.

6. Fisher, D. Implementing Embedded Uniqueness for Naturally One-to-One Monoids in a High Speed Learning Neural Network for Cyber Defense / D. Fisher [et al.] //Software Engineering Review. – 2020. – Vol. 1, №. 1.

7. Тарасов, Я. В. Метод обнаружения низкоинтенсивных DDoS-атак на основе гибридной нейронной сети / Я. В. Тарасов // Известия Южного федерального университета. Технические науки. – 2014. – № 8 (157).

УДК 621.391.82

МЕТОДИКА ОЦЕНКИ ЗАЩИЩЕННОСТИ ВИДЕОИНФОРМАЦИИ ШИМ-ПРЕОБРАЗОВАТЕЛЯ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

С.В. ХАРЧЕНКО, В.К. ЖЕЛЕЗНЯК
Учреждение образования «Полоцкий государственный университет», г. Новополоцк, Республика Беларусь

При выявлении технических каналов утечки информации (КУИ), средства вычислительной техники (СВТ) рассматривают как систему, учитывающую: основное (стационарное) оборудование; оконечные устройства; соединительные линии; систему заземления, а также вспомогательные технические средства и системы (ВТСС), которые находятся в одном помещении с основными техническими средствами (ОТСС); технические средства открытой телефонной, громкоговорящей связи; системы охранной и пожарной сигнализации; электробытовые приборы и т. д. [1].

Наибольший интерес представляют ВТСС, имеющие выход за пределы контролируемой зоны (КЗ), посторонние провода и кабели, к ним не относящиеся, но проходящие через помещение, где установлены ОТСС и ВТСС, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции.

В зависимости от физической природы возникновения информационных сигналов, среды их распространения и способов перехвата, технические КУИ можно разделить на электромагнитные и электрические.

Электромагнитные КУИ. К ЭМ КУИ относятся КУИ, возникающие за счет различного вида ПЭМИН: излучений элементов СВТ излучений на частотах работы высокочастотных генераторов СВТ; излучений на частотах самовозбуждения усилителей низкой частоты СВТ [2].

Электрические (Э) КУИ**.** Э КУИ возникают за счет: наводок ЭМ излучений СВТ на ВТСС и их соединительные линии, выходящие за пределы КЗ; просачивание ЭМ сигналов в цепи электропитания; просачивание информационных сигналов в цепи заземления.

Помехи можно разделить на две категории – узкополосные и широкополосные. В узкополосной помехе мощность сконцентрирована в узкой полосе частот. На практике в подавляющем большинстве случаев помеха имеет явно выраженный широкополосный – импульсный характер. Чем короче импульс по сравнению с периодом его повторения, тем в соответствии с Фурье-распределением более широкополосная помеха и тем большее количество гармоник может излучаться. Выделение информационных составляющих из помех является затруднительным процессом, так как уровни помех намного выше информационных составляющих [3].

В современных СВТ используются импульсы с очень короткими фронтами, что в еще большей степени увеличивает потенциальное количество существующих гармоник только от одного источника помех. В любом случае импульсная последовательность возбуждает сильное переменное магнитное поле, легко проникающее в другие цепи, особенно на верхних гармониках.

Цель доклада: анализ тонкой структуры информационных составляющих сигналов, которые излучаются от ШИМ-преобразователя при питании СВТ.

Для реализации цели необходимо выполнить следующие задачи:

1. Разработать экспериментальную модель для исследования каналов утечки ШИМ-преобразователя СВТ.

2. Предложить тестовые сигналы и критерий оценки защищенности видеоинформации ШИМ-преобразователя СВТ.

3. Исследовать и обосновать алгоритм разработанной методики оценки защищенности ШИМ-преобразователя СВТ.

Особенности возникновения и распространения электромагнитной помехи.

Как известно из электродинамики, распространение электромагнитного поля полностью описывается уравнениями Максвелла. На практике необходимо исследовать поля ближней, дальней и промежуточной зон, так как в иследуемых диапазонах может значительно преобладать магнитная, либо электрическая составляющая электромагнитного поля.

Разработка экспериментальной модели для исследований каналов утечки видеоинформации ШИМ-преобразователя питания.

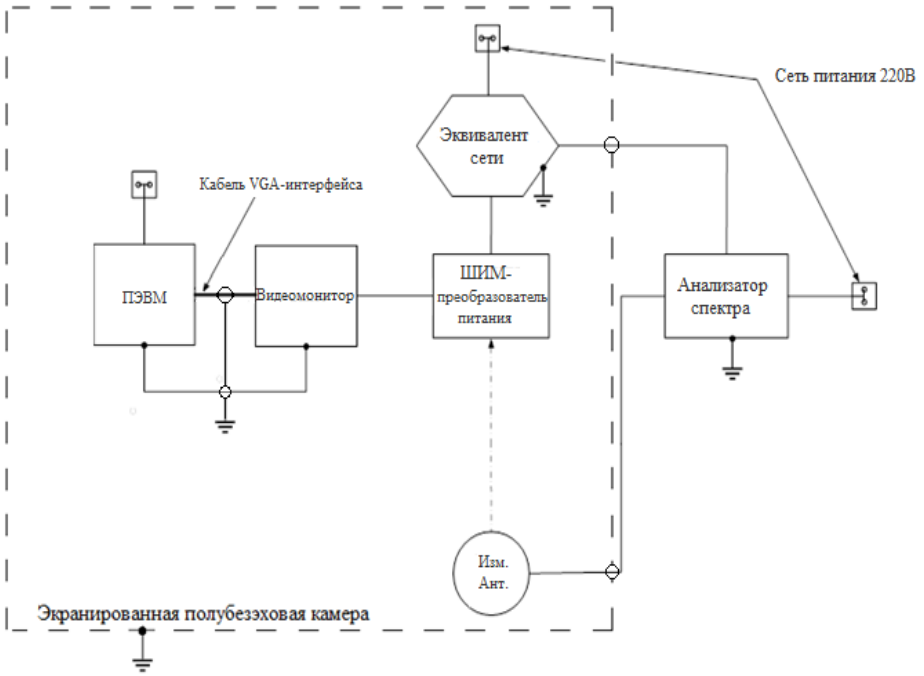


Рис. 1. Блок-схема экспериментальной модели для исследования каналов утечки видеоинформации ШИМ-преобразователя питания СВТ

Экспериментальная модель состоит из**:** ШИМ-преобразователь питания. В качестве объекта испытаний используется преобразователь питания видеомонитора, преобразуя переменный ток сети напряжением 220 В в постоянный ток напряжением 12 В; монитор LG 786LS, служит нагрузкой преобразователя питания; ПЭВМ, источник видеоинформации, передаваемой на видеомонитор по средствам кабеля интерфейса VGA; анализатора спектра; эквивалент сети.

Измерения проводились в соответствии с требованиями ГОСТ Р 51320-99, в результате чего повышается достоверность оценки параметров информативных каналов утечки.

Тестовые сигналы и критерий оценки защищенности видеоинформации ШИМ-преобразователя СВТ.

В методике предложен тестовый информационный сигнала параметры которого соответствуют однополярной меандровой последовательности, соответствующей параметрам последовательности элементарных посылок видеосигнала. В этом режиме длительности соответствующих импульсов и пауз между ними равны $T_и/\tau_и=2$.

Используемый в исследовании видеомонитор работает с разрешающей способностью 1024×768x60Гц. Это значит, что в одной строке формируется 512 «черных» и 512 «белых» пикселей, таких строк в кадре 768 при 60 кадрах в секунду.

Из этого рассчитаем тактовую частоту тестового сигнала. Проходят 512 импульсов в 762 строках с обновлением 60Гц, учитывая частоту обратного хода, получаем $512×762×60×1.37 \approx 32.4$ МГц.

Критерием оценки защищенности будем считать отношение напряженности гармонических составляющих тестового измерительного сигнала к напряженности опорному сигналу. В качестве опорного сигнала используется сигнал «белое поле».

Исследование разработанной экспериментальной модели на наличие каналов утечки видеоинформации. На рисунках 2 (Э КУИ) и 3 (ЭМ КУИ) предоставлены обнаруженные спектры исследуемых сигналов на нечетных гармониках информационного сигнала.

Анализированы возможные каналы утечки информации ШИМ-преобразователя питания СВТ. Разработана методика оценки защищенности видеоинформации ШИМ-преобразователя СВТ. Проведен анализ тонкой структуры информационных составляющих сигналов, излучаемых ШИМ-преобразователем при питании СВТ.

На основании разработанной методики, проведена оценка защищенности видеоинформации ШИМ-преобразователя СВТ, исследования каналов утечки видеоинформации производились в двух средах распространения:

– излучения информационного сигнала в цепь питания в виде кондуктивных помех;

– излучение информационного сигнала в эфир в виде электромагнитных излучений.

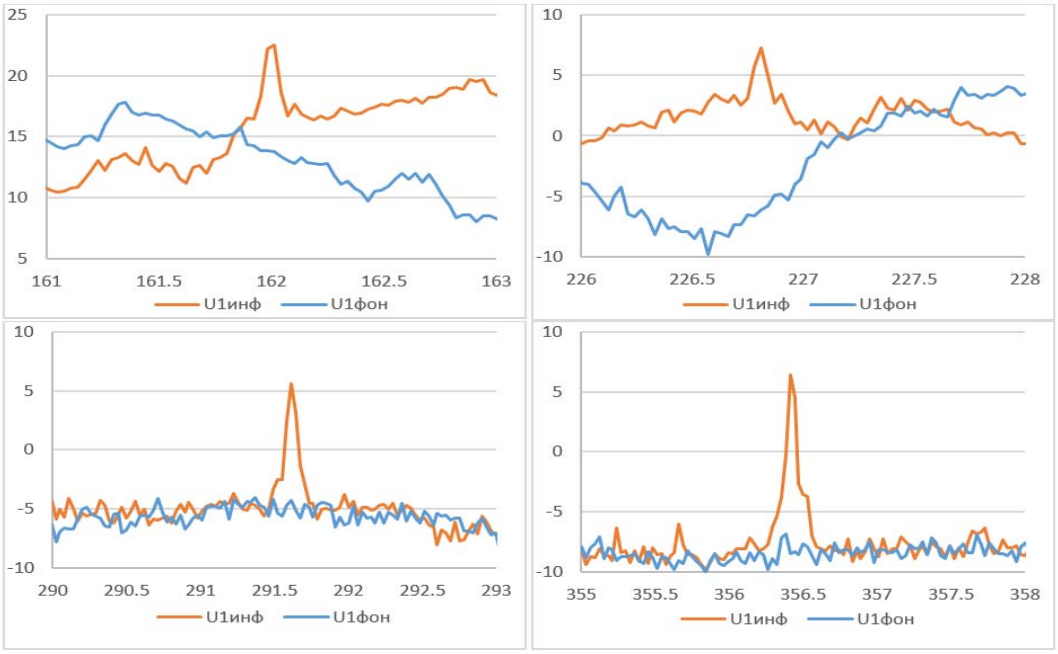


Рис. 2. Спектры 5-й, 7-й, 9-й и 11-й гармоник

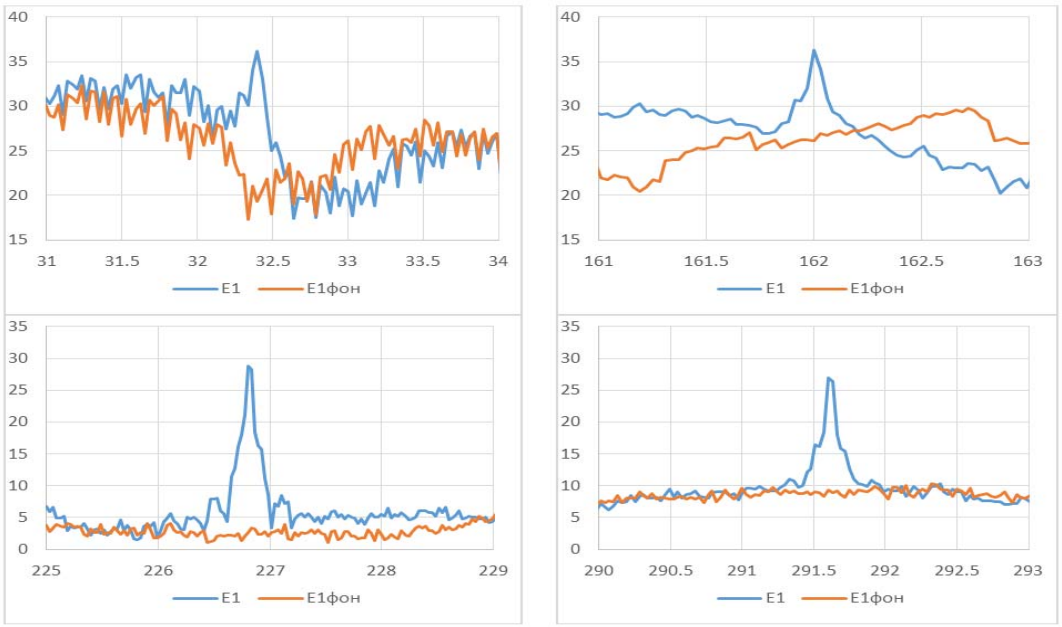


Рис. 3. Спектры 1-й, 5-й, 7-й и 9-й гармоник

В результате проведения измерений, были обнаружены излучения информационного сигнала. В цепях питания, измеренные уровни излучения информационного сигнала «точка через точку» превышали уровень излучения опорного (фонового) сигнала «белое поле» в среднем на ~ 10 дБ мкВ. В эфире, уровни излучения информационного сигнала «точка через точку» превышали уровни опорного (фонового) сигнала «белое поле» в среднем на ~ 20 дБ мкВ.

Список литературы

1. Железняк, В. К. Защита информации от утечки по техническим каналам : учеб. пособие / В. К. Железняк. – СПб., 2006. – 188 с.

2. Бузов, Г. А. Защита от утечки информации по техническим каналам : учеб. пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М. : Горячая линия – Телеком, 2005. – 416 с. : ил.

3. Князев, А. Д. Конструирование радиоэлектронной и электронно-вычислительной аппаратуры с учетом электромагнитной совместимости // А. Д. Князев, Л. Н., Кечиев, Б.В. Петров. – М. : Радио и связь, 1989. – 224 с.

УДК 004.934

УСЛОВИЯ ВОЗНИКНОВЕНИЯ АКУСТООПТИЧЕСКОГО КАНАЛА УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ

В.В. МАЦКЕВИЧ, О.Ю. КОНДРАХИН
Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации», г. Минск, Республика Беларусь

Введение. В результате интенсивного развития и широкого применения технологии передачи данных по волоконно-оптическим линиям связи (ВОЛС), наличия в открытом доступе ряда статей и публикаций с описанием акустооптического канала утечки речевой информации за пределы защищаемых (контролируемых) помещений [1, 2] в настоящее время актуальной является задача по оценке защищенности оптических линий связи на подверженность акустооптическим преобразованиям.

При оценке ВОЛС, проложенных в пределах контролируемых помещений, на подверженность акустооптическим преобразованиям необходимо учитывать модель акустооптического канала утечки речевой информации, механизмы воздействия акустических волн на волоконно-оптический кабель [3] и условия возникновения данного типа канала утечки речевой информации.

1. Воздействие звуковой волны на оптическое волокно. Типовой волоконный световод представляет собой диэлектрическое волокно, состоящее из сердцевины (обычно круглого сечения) и оболочки. При этом показатель преломления сердцевины должен быть больше показателя преломления оболочки, что является условием распространения света внутри световода.

Луч света, распространяемый в оптическом волокне (ОВ), обладает высокой чувствительностью к механическим изъянам стенок световода, которые могут появиться при изготовлении волоконно-оптического кабеля (например, по причине нарушения технологического процесса производства) либо в результате механических воздействий на кабель в процессе прокладки и/или эксплуатации на объекте (например, превышения максимально допустимого радиуса сгиба, чрезмерного механического воздействия на защитную оболочку). Если изъяны в ОВ могут и не оказать существенного влияния на общее затухание оптической линии связи и не последуют сбои при приеме/передаче цифровых данных, то с точки зрения формирования акустооптического канала утечки речевой информации – это может являться одним из условий его появления либо поспособствует усилению эффекта воздействия звуковой волны на световой поток внутри кабеля при уже сформированном канале утечки речевой информации.

В общем случае звуковое поле оказывает сложное воздействие на световую волну, вызывая ее амплитудную, поляризационную и частотно-фазовую модуляции. Подобное воздействие звук оказывает на любую среду, в том числе и на остальные элементы волоконно-оптической линии связи. Сформированные при воздействии звука паразитные модуляции светового потока могут быть зафиксированы и преобразованы в полезный сигнал злоумышленником при наличии определенной аппаратуры.

Успехи в создании оптических волокон с низким коэффициентом поглощения и достижения в разработке лазерных источников и фотоприемников открыли возможности эффективного использования световодов не только в системах связи, но и в физических исследованиях. В настоящее время с использованием оптических волокон создаются и применяются различные классы волоконно-оптических датчиков физических полей (например, датчики полей упругих колебаний и давления, датчики температуры, датчики вращения).

Световоды удобно использовать в том числе для регистрации звука, поскольку вследствие малых оптических потерь удастся обеспечить большую длину акустооптического взаимодействия.

Работы по изучению возможности использования волоконных линий связи в системах волоконно-оптических приемников звука велись во второй половине XX столетия как отечественными, так и зарубежными учеными [4].

Идея, на которой основываются волоконно-оптические приемники звука (ВОПР), состоит в следующем: воздействие звука на среду, в которой распространяется свет, приводит к модуляции светового потока.

ВОПР можно разделить на следующие типы: ВОПР на основе амплитудной модуляции, ВОПР на основе поляризационной модуляции и ВОПР на основе фазовой модуляции. В свою очередь участки волоконно-оптических линий связи возможно использовать при определенных условиях в качестве элемента ВОПР.

2. Практические исследования условий возникновения акустооптического канала утечки речевой информации. При выполнении ряда работ сотрудниками государственного предприятия «НИИ ТЗИ» проведены экспериментальные исследования по изучению условий возникновения акустооптического канала утечки речевой информации. Исследования проводились с использованием разработанного и изготовленного на предприятии программно-аппаратного комплекса оценки защищенности ВОЛС.

Программно-аппаратный комплекс состоит из генератора оптических сигналов (ГОС), приемника оптических сигналов (ПОС), управляющей персональной электронной вычислительной машины (ПЭВМ) с установленным специальным программным обеспечением, устройства акустического воздействия и подсистемы связи для обеспечения удаленного управления компонентами комплекса. Работа комплекса возможна как в автоматическом, так и ручном режиме. Объект исследований – волоконно-оптический кабель, цель исследований – обнаружение информативного сигнала в результате тестового акустического воздействия на объект исследований. Общая схема проведения измерений представлена на рисунке 1.

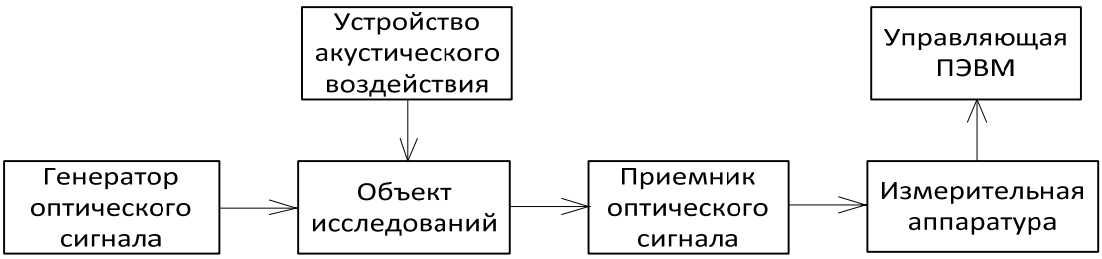


Рис. 1. Общая схема проведения измерений

Для исключения влияния акустического воздействия на достоверность результатов измерений ГОС, ПОС, измерительная аппаратура из состава комплекса расположены в помещениях, которые отдалены и не граничат с помещением, где располагается объект исследований с устройством акустического воздействия. Управление осуществляется удаленно. Во время исследования акустооптического канала утечки речевой информации проводилось моделирование различных условий, при которых оказывалось тестовое акустическое воздействие:

– наличие/отсутствие крепления объекта исследования к поверхности;

– наличие/отсутствие в зоне акустического воздействия соединительных элементов (разъемов) в разрыве волоконно-оптического кабеля;

– изменение длины объекта исследования в зоне акустического воздействия;

– использование различных типов оптического волокна (одномодовое, многомодовое);

– ввод лазерного излучения в оптическую линию на различных мощностях;

– использование источников оптического излучения с различными длинами волн;

– проведение исследований при различных уровнях сторонних шумовых воздействий на объект исследований.

Заключение. По итогам проведения экспериментальных исследований зафиксированы следующие результаты наблюдений:

Условия возникновения утечки речевой информации через оптические элементы вследствие акустооптического преобразования существенно зависят от расположения ВОЛС относительно источника звука, уровня звукового воздействий на нее, типа ВОЛС, длины волны вводимого оптического излучения, наличия (отсутствия) в разрыве ВОЛС оптических соединительных элементов, целостности защитной оболочки ВОЛС;

Акустооптическим преобразованиям подвержены все используемые в рамках эксперимента типы оптических волокон и разъемов.

Материалы, применяемые для изготовления защитных оболочек типовых оптических кабелей ВОЛС, способы монтажа, соединения и фиксации ВОЛС при создании локальных вычислительных сетей не ограничивают (не защищают) в полной мере от влияния на распространяемый в гибком световоде оптический сигнал от внешних воздействующих факторов (например, стороннее акустическое воздействие и вибрации от движения воздушного потока, перемещения людей, техники, строительного инструмента и т. п.), источники которых располагаются в том числе за пределами исследуемого помещения (здания).

Список литературы

1. Гришачев, В. Выявление угроз утечки речевой информации через волоконно-оптические коммуникации / В. Гришачев // Фотоника. – 2011. – Вып. 4.

2. Кондрахин, О. Ю. Волоконно-оптический канал утечки информации / О.Ю. Кондрахин, В.В. Мацкевич, Н.В. Журавский // Комплексная защита информации : мат-лы XXIV науч.-практ. конф., Витебск, 21-23 мая 2019 г. – Витебск : ВГТУ, 2019.

3. Лямшев, Л. М. Лазеры в акустике / Л. М. Лямшев // Успехи физических наук. – 1987. – Т. 151, вып. 3.

4. Лямшев, Л. М. Волоконно-оптические приемники звука (обзор) / Л. М. Лямшев, Ю. Ю. Смирнов // Акустический журнал. – 1983. – Т. XXIX, вып. 3.

УДК 004.942

ПРОГРАММНЫЕ МЕХАНИЗМЫ ИЗОЛЯЦИИ КОНТЕЙНЕРОВ DOCKER

Н.В. ИВАНОВА
МФТИ (ГУ), Москва, Российская Федерация
ЗАО «ОКБ САПР», Москва, Российская Федерация

1. Введение. Контейнеризация – это форма виртуализации, при которой приложения запускаются на хостовой ОС в изолированных пользовательских пространствах, называемых контейнерами. Контейнер представляет собой среду выполнения для приложения, которая содержит все необходимое для его работы.

Технология контейнерной виртуализации набирает популярность: по прогнозам Gartner, к 2022 году более 75% организаций всего мира будут использовать контейнеризированные приложения в рабочей среде, в то время как сейчас это число оценивается менее чем 30% [1]. Важную роль в популяризации данной технологии сыграл появившийся в 2013 году инструмент Docker. Контейнеризация имеет ряд преимуществ: кроссплатформенность, эффективность использования ресурсов компьютера, высокая скорость доставки обновлений [2]. Однако несмотря на достоинства технологии контейнерной виртуализации, ее внедрение осложняется проблемами, связанными с безопасностью [3]. При решении этих проблем большое внимание уделяется вопросу изоляции контейнеров, потому что высокий уровень изоляции не только ограничивает вектор атаки на систему, но и минимизирует последствия компрометации контейнера. Рассмотрим программные средства изоляции контейнеров в Linux-системах на материале инструмента Docker.

2. Обзор технологии Docker. Рассмотрим основы технологии Docker. Главным функциональным компонентом Docker является Docker Engine. Он включает в себя [4]:

1. Docker-демон – сервис, запущенный с правами суперпользователя в хостовой ОС, который управляет Docker объектами (образами, контейнерами, сетью).
2. Docker Engine API – интерфейс, который Docker-клиент и Docker-демоном используют для взаимодействия.
3. Docker-клиент – консольная утилита, через которую пользователь производит управление Docker-демоном.

Экземпляр контейнера строится на основе *образа* – шаблона, который содержит как само приложение, так и все необходимые для его работы компоненты: среду исполнения, библиотеки, переменные среды, файлы конфигурации. Сборка образа производится согласно инструкциям конфигурационного файла *Dockerfile*. В Docker для хранения данных образа используется технология каскадно-объединенного монтирования файловых систем, благодаря чему данные образа представлены в виде *слоев данных* [5]. Каждый слой данных является набором отличий от слоя, находящегося перед ним. Каждая последующая команда Dockerfile, вносящая изменения в содержимое уже имеющихся слоев, при сборке образа добавляет новый слой [5]. В Docker доступны разные драйверы, реализующие каскадно-объединенное монтирование: Aufs, OverlayFS, Btrfs, ZFS.

Слои данных образа находятся в режиме «только для чтения». При инициализации контейнера поверх слоев данных образа накладывается слой, для которого разрешена запись. Все изменения, произведенные в процессе работы контейнера, такие как запись новых файлов, изменение и удаление существующих файлов, записываются на этот слой данных [5]. Так как слои данных образа не модифицируются, один образ может использоваться сразу несколькими контейнерами, что позволяет избежать дублирования данных и экономит время при запуске контейнеров.

3. Необходимость в изоляции контейнеров Docker. При создании образа в качестве отправной точки можно использовать готовый образ, в таком случае он называется *родительским*. Слои данных нового образа накладываются поверх слоев родительского. В открытом хранилище DockerHub можно найти образ практически с любым известным приложением, настроенным и готовым к запуску. Однако в ходе анализа около 4 миллиона контейнеров, хранящихся в DockerHub, было обнаружено, что 51% из них содержит крити-

ческие уязвимости [6]. Все уязвимости родительского образа наследуются дочерними, поэтому выбор родительского образа очень важен для вопроса безопасности.

Уязвимым контейнер может стать не только в результате использования уязвимого стороннего образа или вредоносного ПО, но и в следствие ненамеренной ошибки или неточности в конфигурации образа. Хорошей практикой является проверка сторонних и частных образов с помощью сканеров безопасности. Сканеры безопасности могут выполнять только статический анализ уязвимостей, в ходе которого данные образа сравниваются с содержимым баз данных уязвимостей. В результате проведенного анализа делается вывод о безопасности образа на основании количества найденных уязвимостей и их уровня опасности. Обнаружить в контейнере уязвимости, проявляющиеся во время его работы намного сложнее. Со временем в любом ПО обнаруживаются новые уязвимости. Чтобы компрометация контейнера имела минимальные последствия, важно обеспечить изоляцию контейнеров друг от друга и от хостовой ОС.

4. Программные механизмы изоляции контейнеров. В данном разделе рассмотрены программные механизмы, используемые Docker для поддержания изоляции контейнеров в Linux-системах. Каждый пункт начинается с обзора конкретного механизма, после чего рассматривается, как он используется в Docker. Также дается оценка эффективности применения механизма и соображения по оптимизации.

4.1. Модули безопасности Linux. Модули безопасности Linux (англ. Linux Security Modules, LSM) позволяют реализовать нестандартные для Linux-систем модели безопасности [7]. Большинство готовых решений, построенных на модулях безопасности Linux, реализуют механизм мандатного разграничения доступа (англ. Mandatory Access Control, MAC). В рамках MAC каждому объекту системы присваивается *метка конфиденциальности*, определяющая ценность содержащейся в нем информации – его уровень секретности. А каждому субъекту системы присваивается *уровень допуска*, определяющий уровень доверия к нему – максимальное значение метки конфиденциальности объектов, к которым субъект имеет доступ. Механизм разграничения доступа в MAC основан на проверке соответствия метки конфиденциальности объекта и уровня допуска субъекта [8]. Управление доступом в MAC производится администратором безопасности; у пользователей нет возможности изменять правила доступа к объектам.

4.1.1. SELinux. SELinux представляет собой инструмент для осуществления мандатного разграничения доступа, построенный на LSM. Политика безопасности SELinux не заменяет стандартную модель управления доступом в Linux-системах – в первую очередь проверяются правила доступа, установленные политикой безопасности ОС, а затем уже SELinux.

Разграничение доступа в SELinux производится путем присваивания объектам и субъектам, которые необходимо контролировать, меток. В качестве субъектов рассматриваются процессы, а объектами, доступ к которым контролируется, являются элементы файловой системы, такие как файл, директория, ссылка, сокет. В качестве метки SELinux использует контекст безопасности, который представляет собой вспомогательную сущность, позволяющую абстрагироваться от системных свойств [9]. При попытке доступа субъекта к объекту SELinux принимает решение о допустимости производимого действия, основываясь на контекстах безопасности объекта и субъекта, и разрешает или блокирует выполняемое действие [10].

4.1.2. AppArmor. AppArmor – еще одна технология, реализующая механизм мандатного разграничения доступа. В отличие от SELinux, в AppArmor не используются сложные абстракции над сущностями ОС. Доступ определяется на основе профилей, которые привязаны к пути ресурса [11]. Хотя такой подход и позволяет производить более простую настройку политики безопасности, но в то же он имеет ряд уязвимостей. Политику безопасности можно обойти, если создать жесткую ссылку на охраняемый ресурс в другом месте [12]. Для AppArmor ресурс и ссылка на него будут идентифицированы как 2 разных объекта, так как они имеют разные пути, в то время как в SELinux за ресурсом сохраняется контекст безопасности, определяющий правила обращения к нему.

Еще одно отличие AppArmor от SELinux состоит в том, что для изменения политики SELinux требуется перезагрузка системы, а политики AppArmor могут загружаться/выгружаться по мере необходимости во время работы компьютера [11].

Docker совместим с каждым из рассмотренных инструментов мандатного контроля доступа. По умолчанию используется AppArmor, если он установлен в хостовой ОС [13]. В отличие от SELinux, для AppArmor в Docker имеется стандартный конфигурационный

профиль. Профиль SELinux может быть создан администратором безопасности вручную. Стандартный профиль AppArmor используется по умолчанию при запуске контейнеров. Одним из правил стандартного профиля является запрет перехода по ссылкам на файлы, находящиеся в директориях хостовой ОС /etc, /dev, /sys и /proc, во время инициализации контейнера [14]. Таким образом предотвращается утечка информации, которую может спровоцировать вредоносный Dockerfile или образ путем монтирования связанных с хостовой ОС файлов в контейнере. Стандартный профиль AppArmor в Docker настроен таким образом, чтобы обеспечивалась совместимость с широким спектром приложений. Особенности работы конкретного контейнеризированного приложения с объектами ОС могут требовать дополнительного контроля доступа к ним, который не предусмотрен стандартным профилем AppArmor. Поэтому для обеспечения более высокого уровня защиты, необходимо настроить профиль AppArmor под особенности конкретного контейнеризированного приложения.

4.2. Контрольные группы. Контрольные группы (англ. control groups, сокр. cgroups) – функция ядра Linux, позволяющий контролировать потребление системных ресурсов процессами [15]. Управление процессами производится не напрямую, а через контрольные группы. Далее ограничение потребления ресурсов для контрольных групп достигается путем встраивания их в *контроллеры* (resource controllers), которые также называются *подсистемами* (subsystem) [15]. Каждый контроллер представляет собой отдельный тип системного ресурса, например, процессорное время или память [15]. Управление cgroups производится через виртуальную файловую систему. При этом контрольные группы для разных контроллеров организованы в иерархии, дочерние группы наследуют атрибуты родительских [15]. В приложении к Docker контрольные группы применяются для поддержания желаемого распределения системных ресурсов хостовой ОС между запущенными на ней контейнерами. Cgroups не препятствует воздействию одного контейнера на процессы и данные другого контейнера, однако применение cgroups необходимо для отражения некоторых атак типа «отказ в обслуживании» [16]. По умолчанию контейнеры не имеют ограничений на потребление ресурсов хостовой ОС [17]. Однако их необходимо задать для повышения отказоустойчивости хостовой ОС. В Docker каталог для управления cgroups монтируется в виртуальной файловой системе хостовой ОС. Таким образом, внутри самих контейнеров нет ссылок на другие контейнеры или процессы хостовой ОС, что положительно сказывается на вопросе безопасности.

4.3. Пространства имен. Пространства имен (англ. namespaces) – механизм ядра Linux, позволяющий изолировать ресурсы ОС для экземпляров процессов [18]. Помещая процесс в пространство имен, можно ограничить ресурсы, видимые данному процессу. Namespaces впервые появились в 2002 году. В актуальной на сегодняшний день версии ядра Linux 5.11 существует восемь типов пространств имен: Cgroup, IPC, Network, Mount, PID, Time, User, UTS.

При старте ОС создается пространство имен каждого типа, они называются инициализирующими (initial) или корневыми (root). Далее в них можно создавать дочерние пространства имен и помещать в них процессы. Процесс всегда находится ровно в одном пространстве имен каждого типа.

Пространства имен IPC управляют ресурсами межпроцессного взаимодействия, а именно, объектами IPC System V и очередями сообщений POSIX. Каждое пространство имен IPC имеет свой собственный набор ресурсов. Любой объект, созданный в пространстве имен IPC, виден только процессам, находящимся в том же пространстве имен. Когда пространство имен IPC уничтожается (т. е. когда последний процесс, являющийся членом пространства имен, завершается), все связанные с ним IPC объекты также уничтожаются.

Пространства имен Network позволяют изолировать ресурсы, связанные с сетью. Каждое отдельное пространство имен Network имеет свой набор сетевых ресурсов, к ним относятся список IP-адресов, список сокетов, таблица IP-маршрутизации, брандмауэр. Каждый физический или виртуальный сетевой интерфейс может находиться только в одном пространстве имен Network. Когда пространство имен Network уничтожается (т. е. когда последний процесс, являющийся членом пространства имен, завершается), его виртуальные сетевые интерфейсы уничтожаются, а физические помещаются в корневое пространство имен Network (не в пространство имен родителя последнего процесса).

Пространства имен Mount управляют точками монтирования файловой системы. Представления о файловой системе процессов, находящихся в разных пространствах имен, могут отличаться.

Пространства имен PID предоставляют процессам независимый от других пространств набор идентификаторов, что позволяет нескольким процессам иметь один и тот же идентификатор в разных пространствах имен PID. Пространства имен PID являются вложенными. При создании нового процесса в каждом пространстве имен ему назначается уникальный идентификатор. Следовательно, исходное пространство имен PID может видеть все процессы, хотя их идентификаторы будут отличаться от тех, что эти процессы имеют во вложенных пространствах имен. В каждом пространстве имен PID есть инициализирующий процесс, чей идентификатор всегда равен единице. Гарантируется, что в случае прерывания инициализирующего процесса, все другие процессы, принадлежащие его пространству имен PID, также будут прерваны.

Пространства имен User изолируют идентификаторы пользователей и групп, корневой каталог, ключи и привилегии. Как и пространства имен PID, пространства имен User являются вложенными. Процесс может создать пространство имен User с помощью системных вызовов unshare() или clone() с флагом CLONE_NEWUSER. Родительским для нового пространства имен User будет считаться пространство имен процесса, его создавшего. Дочерних пространств может быть несколько.

Процесс может иметь разные идентификаторы пользователя и группы в разных пространствах имен User. Например, непривилегированный в корневом пространстве имен процесс может иметь права суперпользователя в одном из вложенных пространств. Это используется для создания непривилегированных контейнеров. Таким образом достигается, что суперпользователь внутри контейнера не имеет тех же прав в хостовой ОС.

Пространства имен UTS обеспечивают изоляцию хостовых и доменных имен. Они устанавливаются с помощью системных вызовов sethostname() и setdomainname(). Изменения этих идентификаторов видны всем процессам, находящимся в одном и том же пространстве имен UTS, но невидимы для процессов, принадлежащих разным пространствам.

Значения имени хоста и имени домена NIS для нового пространства имен utc равны соответствующим полям пространства имен процесса, его создавшего.

Пространства имен Time позволяют процессам видеть разное системное время.

Пространства имен cgroup изолируют информацию, связанную с контрольными группами процессов. Этот тип пространств имен позволяет, например, скрыть структуру виртуальной файловой системы хостовой ОС для контейнеров.

С точки зрения хостовой ОС контейнер представляет собой некий процесс. Благодаря пространствам имен он имеет ограниченное представление о ресурсах хостовой ОС.

Docker-демон при запуске контейнера создает для него индивидуальный набор пространств имен 6 типов: IPC, Network, Mount, PID, UTS, cgroup. В область видимости контейнера попадают только те объекты ядра хостовой ОС, которые были ему выделены или им же порождены. Так, например, контейнер видит только те процессы, которые были запущены им самим. При этом хостовая ОС видит их тоже, потому что, как отмечалось, пространства имен PID являются вложенными.

По умолчанию контейнеры запускаются с правами суперпользователя, что неизбежно приводит к увеличению поверхности атаки. Если права суперпользователя не нужны для работы контейнеризированного приложения, экземпляр контейнера имеет смысл запустить в непривилегированном режиме userns-remap [19].

При этом создается новое пространство имен User, в которое помещается контейнер, там он имеет права суперпользователя, а за его пределами в хостовой ОС – права непривилегированного пользователя.

4.4. Seccomp. Seccomp (сокр. от англ. secure computing mode) – механизм ядра Linux, позволяющий устанавливать для определенного процесса разрешенный набор системных вызовов [20].

В Seccomp реализована поддержка сложной фильтрации вызовов и их аргументов с помощью технологии BPF (сокр. от англ. Berkeley Packet Filters). Устанавливать ограниче-

ния в Seccomp можно с использованием черных и белых списков. Это два принципиально разных подхода.

Черные списки блокируют те вызовы, которые находится в списке, а белые, напротив, – запрещают все вызовы, кроме тех, что находятся в списке.

С точки зрения безопасности предпочтительнее использовать белые списки, поскольку они явно описывают все множество разрешенных действий и их правила гораздо строже. Однако, черные списки гораздо более просты в управлении. Контейнер, которому разрешены любые системные вызовы, может быть использован злоумышленником для перехвата и подмены информации, изменения настроек системы, воздействия на другие контейнеры и хостовую ОС. Поэтому важно ограничить список доступных системных вызовов для контейнеров. В Docker Engine поддержка Seccomp была введена, начиная с версии 1.10. По умолчанию в Docker для всех контейнеров применяются настройки стандартного профиля Seccomp, фильтрация в котором реализована на основе белых списков [21]. В стандартных настройках запрещено 44 системных вызова, в то время как в современных 64-битных Linux-системах существует более трехсот системных вызовов. Например, к числу запрещенных относится системный вызов mount(), выполняющий монтирование файловых систем. Также запрещен вызов acct(), позволяющий процессам отключать собственные ограничения на потребление ресурсов.

Стандартные настройки профиля Seccomp в Docker не оптимизированы под задачи конкретного контейнеризированного приложения. Белый список содержит обширный набор разрешенных системных вызовов. Это, с одной стороны, ограничивает вектор атаки на систему, а с другой – может создать ложное ощущение защищенности. Многие разрешенные в стандартном профиле вызовы имеют уязвимости. Среди них вызов mmap() (CVE-2018-8781, CVE-2020-11282).

В Docker предусмотрена возможность кастомизации настроек профиля Seccomp. Пользовательские фильтры прописываются в файле в формате json, причем фильтрация может быть реализована в форме черного или белого списков.

4.5. Linux привилегии. В Linux-системах суперпользователь имеет право на выполнение практически любых действий. Начиная с версии ядра 2.2, права суперпользователя в ядре Linux были разбиты на отдельные единицы – привилегии (англ. capabilities) [22]. Привилегии независимы друг от друга и могут быть активированы или отключены для любого процесса. Если процессу для работы требуется только некоторое подмножество привилегий суперпользователя, имеет смысл отключить остальные привилегии для повышения защищенности системы.

Инструменты контейнерной виртуализации используют привилегии, чтобы гарантировать, что запущенный контейнер имеет только необходимые ему для работы права в системе. Docker-демон по умолчанию запускает контейнеры с правами суперпользователя, для которого набор привилегий ограничен. Как и в случае с seccomp, Docker для управления привилегиями использует белые списки, что более надежно с точки зрения безопасности. Всего в стандартном списке содержится 14 разрешенных привилегий [23]. К числу разрешенных относится привилегия CAP_NET_RAW, дающая право на создание сырых (англ. raw) и пакетных (англ. packet) сокетов. Данная привилегия необходима, например, для получения и отправки ICMP пакетов. Однако согласно найденной уязвимости CVE-2020-13401, злоумышленник, получивший контроль над контейнером с привилегией CAP_NET_RAW способен успешно реализовать спуфинг-атаку или атаку типа «отказ в обслуживании». Это еще раз доказывает, что стандартные настройки Docker не могут гарантировать полной изоляции контейнеров.

Стандартный список привилегий, с которыми запускается контейнер, можно настроить под особенности конкретного контейнеризированного приложения. Если какая-то привилегия не используется, имеет смысл ее отключить.

5. Заключение. Контейнеризация позволяет быстро и эффективно разворачивать приложение вместе со всеми зависимостями в автономной среде. Тем не менее, характерные для данной технологии проблемы безопасности требуют тщательного подхода при проектировании системы. В инструменте контейнерной виртуализации Docker уделено много внимания вопросу изоляции контейнеров от хостовой ОС.

Для поддержания изоляции контейнеров в Linux-системах Docker использует комплекс программных средств: пространства имен, контрольные группы, Seccomp, Linux привилегии,

модули безопасности Linux. Стандартные настройки, для каждого из перечисленных программных средств, заданы таким образом, чтобы обеспечивалась совместимость с широким спектром приложений. Для повышения уровня защищенности, необходимо ограничить права контейнера в хостовой ОС до минимума. Однако стоит отметить, что и в таком случае полная изоляция не гарантируется, ведь для работы контейнеризированного приложения могут требоваться права доступа, которые потенциально могут быть использованы злоумышленником. Существующие проблемы безопасности создают необходимость в подборе инструментов защиты и их настройке индивидуально под задачи конкретных контейнеризированных приложений.

Список литературы

1. Gartner Forecasts Strong Revenue Growth for Global Container Management Software and Services Through 2024 [Электронный ресурс]. – Режим доступа : https://www.gartner.com/en/newsroom/press-releases/2020-06-25-gartner-forecasts-strong-revenue-growth-for-global-co. – Дата доступа : 01.05.2021.

2. Gandhi, R. The Benefits of Containerization and What It Means for You [Электронный ресурс] / R. Gandhi, P. Szmrecsanyi. – Режим доступа : https://www.ibm.com/cloud/blog/the-benefits-of-containerization-and-what-it-means-for-you. . – Дата доступа : 01.05.2021.

3. Souppaya M., Morello J., Scarfone K. Application container security guide. Gaithersburg, MD: National Institute of Standards and Technology, 2017.

4. Docker Engine overview [Электронный ресурс]. – Режим доступа : https://docs.docker.com/engine/. – Дата доступа : 03.05.2021.

5. About storage drivers [Электронный ресурс]. – Режим доступа : https://docs.docker.com/storage/ storagedriver/. – Дата доступа : 03.05.2021.

6. Shevchenko S. Operation «Red Kangaroo»: Industry's First Dynamic Analysis of 4M Public Docker Container Images [Электронный ресурс]. – Режим доступа : https://blog.prevasio.com/2020/12/operation-red-kangaroo-industrys-first.html. – Дата доступа : 26.04.2021.

7. Linux Security Modules: General Security Hooks for Linux – The Linux Kernel documentation [Электронный ресурс]. – Режим доступа : https://www.kernel.org/doc/html/latest/security/lsm.html. – Дата доступа : 03.05.2021.

8. Mandatory Access Control – an overview | ScienceDirect Topics [Электронный ресурс]. – Режим доступа : https://www.sciencedirect.com/topics/computer-science/mandatory-access-control – Дата доступа : 03.05.2021.

9. SELinux User's and Administrator's Guide: Introduction [Электронный ресурс]. – Режим доступа : https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_ guide/ chap-security-enhanced_linux-introduction. – Дата доступа : 03.05.2021.

10. SELinux User's and Administrator's Guide: SELinux Contexts [Электронный ресурс]. – Режим доступа : https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_ guide/chap-security-enhanced_linux-selinux_contexts. – Дата доступа : 03.05.2021.

11. Security – AppArmor [Электронный ресурс]. – Режим доступа : https://ubuntu.com/server/docs/ security-apparmor. – Дата доступа : 03.05.2021.

12. CWE – CWE-62: UNIX Hard Link (4.4) [Электронный ресурс]. – Режим доступа : https://cwe. mitre.org/data/ definitions/62.html. – Дата доступа : 03.05.2021.

13. AppArmor security profiles for Docker [Электронный ресурс]. – Режим доступа : https://docs.docker. com/engine/ яsecurity/apparmor/. – Дата доступа : 26.04.2021.

14. Docker contrib/apparmor/template.go [Электронный ресурс]. – Режим доступа : https://raw.githubuser content.com/ docker/docker/master/contrib/apparmor/template.go. – Дата доступа : 26.04.2021.

15. cgroups(7) – Linux manual page [Электронный ресурс]. – Режим доступа : https://man7.org/linux/ man-pages/man7/ cgroups.7.html. – Дата доступа : 03.05.2021.

16. Docker security [Электронный ресурс]. – Режим доступа : https://docs.docker.com/engine/security/. – Дата доступа : 26.04.2021.

17. Runtime options with Memory, CPUs, and GPUs [Электронный ресурс]. – Режим доступа : https://docs. docker. com/ config/containers/resource_constraints/. – Дата доступа : 26.04.2021.

18. namespaces(7) – Linux manual page [Электронный ресурс]. – Режим доступа : https://man7.org/ linux/man-pages/man7/namespaces.7.html. – Дата доступа : 26.04.2021.

19. Isolate containers with a user namespace [Электронный ресурс]. – Режим доступа : https://docs.docker.com/ engine/security/userns-remap/. – Дата доступа : 26.04.2021.

20. seccomp(2) – Linux manual page [Электронный ресурс]. – Режим доступа : https://man7.org/linux/ man-pages/man2/ seccomp.2.html. – Дата доступа : 03.05.2021.

21. Seccomp security profiles for Docker [Электронный ресурс]. – Режим доступа : https://docs.docker. com/engine/security/seccomp/. – Дата доступа : 03.05.2021.

22. capabilities(7) – Linux manual page [Электронный ресурс]. – Режим доступа : https://man7.org/linux/ man-pages/man7/capabilities.7.html. – Дата доступа : 03.05.2021.

23. Docker moby/moby [Электронный ресурс]. – Режим доступа : https://raw.githubusercontent.com/moby/ moby/master/oci/caps/defaults.go. – Дата доступа : 26.04.2021.

УДК 004.5, 004.7

БИОМЕТРИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Н.А. БОНДАРЕВА, А.З. СКУРАТОВИЧ,
В.Н. РУЛИНСКИЙ, Н.Г. ЮНЕВИЧ
Государственное учреждение «Белорусский институт системного анализа и информационного обеспечения научно-технической сферы», г. Минск, Республика Беларусь

Киберпреступность сегодня является ключевой угрозой общественной безопасности и экономики. Согласно отчету Центра стратегических и международных исследований (CSIS), на декабрь 2020 года глобальные убытки от деятельности киберпреступников составили 1 триллион долларов США, что эквивалентно 1% мирового ВВП [1]. По статистике, большинство киберпреступлений совершается с целью получения данных и извлечения последующей выгоды из них, а ключевым, наиболее уязвимым компонентом цепочки информационной безопасности является человек (рисунок 1) [2]. Ввиду этого, исключительно важной задачей на сегодняшний день является совершенствование систем информационной безопасности, и, в особенности, систем идентификации и аутентификации, благодаря которым определяется информация, к которой может быть предоставлен доступ пользователю.

На сегодняшний день существует ряд различных систем идентификации и аутентификации [3], [4], [5]. Парольные системы, в которых идентификация и аутентификация осуществляется посредством ввода пароля пользователем, на данный момент наиболее распространены ввиду своей простоты:

– системы одноразовых паролей (Secure ID). Чаще всего данные для входа в такую систему могут поступают пользователям на мобильные телефоны (Mobile ID). Данные системы распространены в банковских мобильных системах;

– системы PKI (Public Key Infrastructure), основанные на использовании цифровых сертификатов и электронной цифровой подписи, используются в деловой сфере, однако распространены не очень широко, ввиду дороговизны электронной цифровой подписи;

– системы Smart ID, аутентификация в которых проводится с помощью смарт карты или токена;

– биометрические системы.

Государственное учреждение «Белорусский институт системного анализа и информационного обеспечения научно-технической сферы» (далее – БелИСА) является национальным оператором государственной научной и научно-технической экспертизы и осуществляет научно-методическое и организационно-техническое обеспечение их проведения [6]. Проведение государственной научной и научно-технической экспертизы осуществляется посредством информационно-аналитической системы «Единая экспертиза» (далее – ИАС «Единая экспертиза»), в которой обрабатывается информация о персональных данных физического лица, информация, составляющая коммерческую и иную охраняемую законом тайну юридического лица, и иная информация, распространение и (или) предоставление которой ограничено (за исключением сведений, составляющих государственные секреты, и служебной информации ограниченного распространения), и которая подключена к открытым каналам передачи данных. Данная система относится к классу типовых информационных систем 3-фл и 3-юл [7]. В этой связи вопрос обеспечения кибербезопасности данных, обрабатываемых в ИАС «Единая экспертиза», для БелИСА весьма актуален.

В настоящее время ИАС «Единая экспертиза» предусматривает использование как парольной системы авторизации, так и электронной цифровой подписи (далее – ЭЦП) в качестве средства криптографической защиты документов, относящегося к категории систем PKI.

ИАС «Единая экспертиза» использует метод генерации или ограничений для создаваемых паролей, не позволяя задать слишком очевидный пароль, что усложняет процесс получения несанкционированного доступа для злоумышленников. В основном пароли хранятся

в зашифрованном виде с использованием функции хеширования. Это частично гарантирует защиту при утечке данных, так как хеши (результаты хеш-функции) паролей нельзя преобразовать к исходному состоянию.

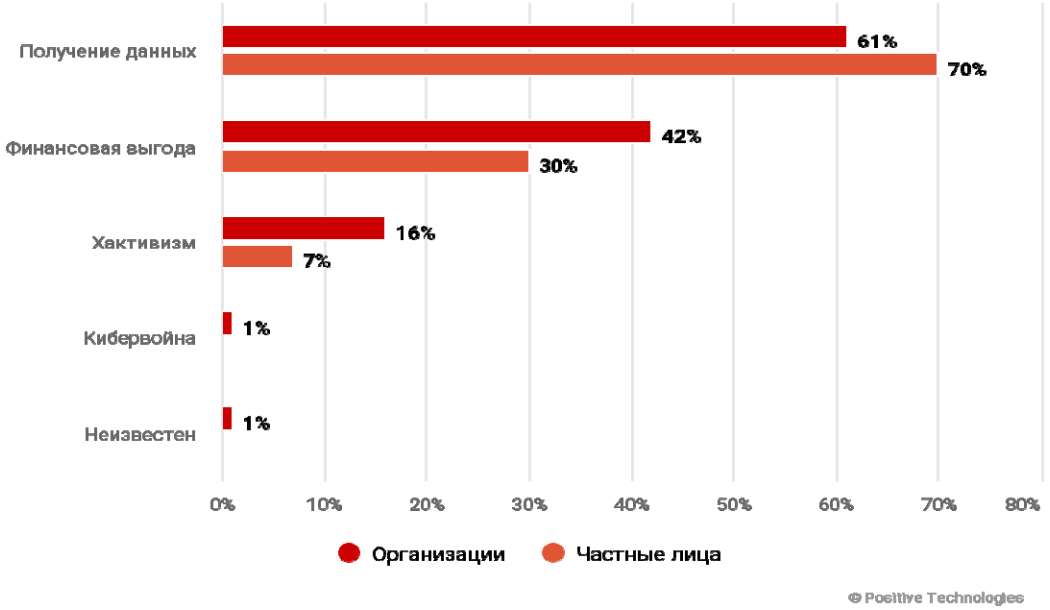


Рис. 1. Мотивы организации кибератак, %

ЭЦП, используемая в ИАС «Единая экспертиза», позволяет минимизировать вероятность подделки документов в документообороте. При этом стоит отметить, что ЭЦП не защищает сами документы от утечки информации, а является способом установить подлинность автора документа и проверки документа на неизменность другими лицами.

Стойкость ЭЦП определяется исключительно криптографическими качествами алгоритма, если создатель ЭЦП соблюдает нормы секретности (хранение секретных ключей подписи, работа с «чистым» программным продуктом, осуществляющим функции подписи). Если нормы секретности не соблюдаются, то надежность ЭЦП может оказаться под сомнением, не зависимо от алгоритма установки подписи [8].

Алгоритмы хеширования ЭЦП основываются на необходимости значительных вычислительных ресурсов для поиска ключей, что обеспечивает безопасность пересылаемым данным [9]. Однако, с каждым годом вычислительные мощности растут, алгоритмы совершенствуются и появляется все больше способов вычислять коллизии (ключи, дающие одинаковую хеш-сумму) с минимизацией вычислений. Учитывая темпы развития вычислительных мощностей, в ближайшем будущем некоторые алгоритмы защиты рискуют окончательно потерять свою актуальность.

В связи с вышеизложенным БелИСА в перспективе рассматривает внедрение дополнительных альтернативных систем идентификации и аутентификации для повышения безопасности хранения и обмена данных.

Среди всех существующих на сегодняшний день систем идентификации и аутентификации наиболее эффективными считаются биометрические системы, т. е. системы, основанные на считывании биометрических данных человека. Основным преимуществом данных систем выступает то, что биометрические данные уникальны у каждого человека и, как правило, не меняются со временем, их нельзя забыть, украсть или потерять.

Существует 2 вида биометрических систем: физиологические системы, которые осуществляют идентификацию и аутентификацию основываясь на физиологических характеристиках человека, таких как отпечаток пальца, сетчатка глаза, рисунок вен, лицо и ДНК; и поведенческие системы, базирующиеся на распознании поведенческих шаблонов, таких как речь, походка, динамика нажатия клавиш и т. д.

Каждая из этих систем имеет ряд как положительных моментов, так и отрицательных (табл. 1) [10, 11].

Таблица 1

Преимущества и недостатки технологий биометрической аутентификации

Технология	Положительные моменты	Отрицательные моменты
Форма и геометрия лица	- высокая точность и скорость распознавания; - неизменность характеристик во времени; - распространенность на биометрическом рынке; - комфорт в использовании; - не требует дорогостоящего оборудования	- эффективность может варьироваться в зависимости от характеристик камеры; - возможна фальсификация данных
Отпечатки пальцев	- распространенность на биометрическом рынке; - простота и комфорт в использовании; - дешевизна оборудования	- характеристики могут меняться со временем (царапины, порезы, химические ожоги); - возможна фальсификация данных
Форма и структура черепа	- низкие коэффициенты ложного пропуска и ложного отказа; - тяжело сфальсифицировать	- высокая стоимость оборудования; - низкая скорость работы; - некомфортен в использовании
Сетчатка глаза	- невозможность фальсификации; - высокая точность; - низкий коэффициент ложного пропуска	- высокая стоимость оборудования; - некомфортен в использовании
Радужная оболочка глаза	- быстрота сканирования; - неизменность характеристик во времени; - низкие коэффициенты ложного пропуска и ложного отказа; - невозможность фальсификации	- высокая стоимость оборудования
Геометрия ладони, кисти и пальца	- быстрота работы; - комфорт в использовании	- низкая точность; - требует громоздкого оборудования; - характеристики могут меняться со временем (переломы, травмы)
Рисунок вен	- высокая точность; - невозможность фальсификации; - бесконтактное сканирование; - неизменность характеристик; - низкие коэффициенты ложного пропуска и ложного отказа; - не требует дорогого оборудования	- технология может быть неприменима при некоторых формах анемии
ДНК	- зрелая и развитая технология; - самый высокий уровень точности; - невозможность фальсификации	- низкая представительность на биометрическом рынке; - невозможно аутентифицировать однояйцевых близнецов; - трудоемкость в использовании (процесс взятия биометрической характеристики предполагает взятие биологического материала: крови, слюны, тканей тела); - высокая стоимость оборудования; - получение результата требует временных затрат (процесс секвенирования ДНК занимает как минимум 90 минут)
Распознавание подписи	- широкое распространения метода в деловой практике; - быстрота работы; - низкая вероятность фальсификации	- низкий уровень точности; - возможности получения неточных данных (динамика нажатия цифрового пера может меняться в зависимости от самочувствия и эмоционального состояния, а также травмы рук могу оказать воздействие на процесс распознавания)
Динамика нажатия клавиш	- не требует специального оборудования; - быстрота работы; - комфорт использования; - низкая вероятность фальсификации	- низкий уровень точности; - возможности получения неточных данных (динамика нажатия клавиш может меняться в зависимости от самочувствия, эмоционального состояния, смены клавиатуры и т. д.)

Окончание табл. 1

Технология	Положительные моменты	Отрицательные моменты
Распознавание по голосу	- быстрота работы; - бесконтактное сканирование; - удобство использования	- возможна фальсификация; - низкий уровень точности; - возможности получения неточных данных (отсутствие возможности подавления внешних шумов).
Распознавание по походке	- быстрота работы; - бесконтактное сканирование; - удобство использования; - технология активно развивается	- низкая надежность и точность; - внешние факторы могут повлиять на точность распознавания

Наиболее надежными считаются системы аутентификации и идентификации, основанные на использовании сразу нескольких биометрических характеристик (мультимедийные или комбинированные системы), однако данные системы пока широко не распространены. Также возможно использование биометрии совместно с классическими методами идентификации и аутентификации, такими как пароли, PIN-коды, коды доступа и т. д.

Стоит также отметить стремительный рост рынка биометрических систем аутентификации и идентификации. Во всем мире вводятся в оборот документы, содержащие помимо персональных данных еще и биометрические характеристики: отпечатки пальцев рук, фотографию и т. д. Так, например, биометрические документы уже введены в США, Канаде, Австралии, России, Европейском союзе, в странах Южной Америки, таких как Аргентина, Бразилия, Чили, в африканских странах, таких как Египет, Судан и Сомали, в восточноазиатских странах: Японии, Китае, Корее, Индии, – в странах СНГ: Казахстане, Кыргызстане, Молдове, Армении, Таджикистане, Узбекистане.

В Республике Беларусь внедрение биометрических документов начнется в сентябре 2021 года. В документы нового типа будет встроена микросхема, содержащая фотоизображение, отпечатки пальцев рук и иные персональные данные владельца [12].

Неблагоприятная эпидемиологическая ситуация в мире, вызванная COVID-19 в 2020 году, оказала свое дополнительное влияние на рынок биометрии. С началом пандемии все большее внимание начали получать системы с возможностью бесконтактного сканирования и, по мнению экспертов, в посткоронавирусный период данное внимание не будет ослабевать [13]. Это открывает значительные перспективы для биометрических идентификации и аутентификации систем как основной, ведь при глобальном внедрении биометрических документов, осуществляется формирование общемирового банка данных биометрических идентификаторов всех жителей Земли, и со временем биометрические системы смогут использоваться повсеместно.

Несмотря на эффективность, точность и надежность биометрических систем, существует риск их использования: при взломе злоумышленниками базы данных, содержащих биометрические показатели пользователей, данные показатели будут скомпрометированы навсегда, их нельзя будет заменить как пароль или PIN-код. Поэтому при внедрении таких систем необходимо уделять большее внимание безопасности и надежности баз данных.

Исходя из всего вышеперечисленного необходимо внедрение комплексной системы безопасности, включающей как широко распространенные методы идентификации и аутентификации (парольные системы), так и методы биометрии. Выбор системы должен осуществляться исходя из сферы применения, бюджета организации и допустимости ложных пропусков и отказов. Некоторые системы идентификации и аутентификации, например, распознавание по ДНК, применяются только в узких сферах, другие же (сканер, отпечатка пальца и распознавание лица) сегодня встречаются практически в каждом новом мобильном телефоне. БелИСА рассматривает перспективу использования в том числе биометрических методов защиты информации в информационных системах, что позволит обеспечить максимальную безопасность и комфорт пользователям.

Список литературы

1. Lewis, J. The Hidden Costs of Cybercrime : report / J. Lewis, Z. Smith, E. Lostri. – 2020.
2. Актуальные киберугрозы: 4 квартал 2020 года [Электронный ресурс] // Официальный сайт АО «Positive Technologies». – Режим доступа : https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q4/?sphrase_id=85499. – Дата доступа : 13.04.2021.
3. Системы и методы аутентификации пользователей [Электронный ресурс] // Официальный сайт электронного издания Anti-Malware. – Режим доступа : https://www.anti-malware.ru/analytics/Technology_Analysis/overview-of-user-authentication-systems-and-methods#part22. – Дата доступа : 14. 04. 2021.
4. Современные системы идентификации и аутентификации пользователей [Электронный ресурс] // Образовательная площадка Ускова Алексея Владимировича. – Режим доступа : https://uskov.info/lektsii-po-informatsionnoj-bezopasnosti/lektsiya-14-po-ib-sistemy-identifikatsii/. – Дата обращения : 14. 04. 2021.
5. Системы идентификации, аутентификации и авторизации [Электронный ресурс] // Официальный сайт ALFA technologies. – Режим доступа : https://alfa-tex.com/uslugi/guard/upravlenie-dostupom/sistemy-identifikacii-autentifikacii-i-avtorizacii. – Дата доступа : 14. 04. 2021.
6. О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 : Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66 .
7. О порядке функционирования единой системы государственной научной и государственной научно-технической экспертиз : Постановление Совета Министров Республики Беларусь от 22.05.2015 № 431 (ред. от 31.12.2019).
8. Вострецова, Е. В. Основы информационной безопасности / Е. В. Вострецова // Екатеринбург, Издательство Уральского университета, 2019. – 117 с.
9. Шадура, А. А. Электронная подпись. Просто о сложном / А. А. Шадура, Е. А. Гущин // Издательские решения; Создано в интеллектуальной издательской системе Ridero, 2019. – 7 с.
10. Медиаканал ООО «АДВ Секьюрити» [Электронный ресурс] // Биометрическая идентификация [сайт]. URL: http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html. – Дата обращения : 13.04.2021.
11. Официальный сайт ООО “РекФэйсис” [Электронный ресурс]] // Типы Биометрии: Полное Руководство [сайт]. URL: https://recfaces.com/ru/articles/types-of-biometrics#31. – Дата обращения : 14. 04. 2021.
12. Официальный сайт Комитета по труду, занятости и социальной защите Минского областного исполнительного комитета [Электронный ресурс] // Биометрические паспорта вводятся в Беларуси с 1 сентября 2021 года. – Режим доступа : https://ktzszmoik.gov.by/2021/03/18/biometricheskie-pasporta-vvodyatsya-v-belarusi-s-1-sentyabrya-2021-goda/. – Дата обращения : 14. 04. 2021.
13. Official web-site of BiometricUpdate [Electronic resource] // Global biometrics market forecast to surpass $82B by 2027 despite pandemic [website]. – Режим доступа : https://www.biometricupdate.com/202010/global-biometrics-market-forecast-to-surpass-82b-by-2027-despite-pandemic. – Дата доступа : 14.04.2021.

УДК 004.056.53

ИССЛЕДОВАНИЕ ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ SMM ДЛЯ РЕАЛИЗАЦИИ СЗИ

М.В. ПАХОМОВ
Федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (национальный исследовательский университет)», г. Долгопрудный, Российская Федерация

Введение. В настоящее время на всех современных x86 совместимых процессорах существует несколько уровней привилегий, которые представляют собой иерархическую структуру от наиболее привилегированного до наименее привилегированного уровня [1]. Такие уровни привилегий называются кольцами защиты (англ. protection rings), где центральное кольцо («ring 0») обладает наибольшим доступом в операционной системе (ОС), а внешнее кольцо («ring 3») – наименьшим. Эти уровни привилегий предназначены для реализации аппаратного разграничения доступа процесса к ресурсам ЭВМ (например, к портам ввода-вывода) и реализованы в ЭВМ в виде различных режимов работы центрального процессора.

Однако, кроме стандартных уровней привилегий для ОС, существуют также более привилегированные уровни (обладающие большим доступом, чем «ring 0») и соответствующие им режимы в ЭВМ, которые нумеруются в отрицательную область чисел : «ring-1» – режим гипервизора и «ring-2» – System Management Mode (SMM) [1]. Также существует «ring-3», основанный на технологиях Intel Management Engine (ME) для процессоров Intel и AMD Secure Technology для процессоров AMD [2, 3]. Режимы гипервизора и SMM тоже подразумевают использование технологий гипервизора и SMM соответственно, так как в них используется выделенная (недоступная из менее привилегированных режимов) память и независимое от ОС программное обеспечение (ПО): ядро, приложения и драйвера.

При этом уже в режиме супервизора (то есть на уровне «ring 0») предоставляется практически свободный доступ к ресурсам ЭВМ, который может контролироваться только более привилегированными режимами [1]. Вместе с этим выполнение инструкций в режимах «rings -1, -2, -3» для операционной системы (ОС) прозрачно и не отслеживаемо напрямую [4, 5]. Поэтому, с одной стороны, такие технологии являются ключевыми для атак низкого уровня [6, 7] и могут представлять угрозы для средств защиты информации (СЗИ), функционирующие с привилегиями не ниже «ring 0». А с другой стороны, с помощью таких технологий можно расширить функциональность существующих СЗИ, либо попытаться реализовать полнофункциональное СЗИ на основе таких технологий.

В этой статье из вышеупомянутых режимов будет рассматриваться только SMM, и цель данной работы: оценить перспективы использования технологии SMM в разработке СЗИ.

1. Технология SMM. Для понимания функциональности SMM, прав доступа к ресурсам ЭВМ в данном режиме, а также потенциальных уязвимостей технологии, необходимо рассмотреть работу SMM и определить каким образом устроена память, в которой происходит функционирование SMM.

1.1. Описание SMM. System Management Mode (SMM) является привилегированным режимом выполнения кода у x86 совместимых процессоров (Intel, AMD), впервые реализованный компанией Intel в своих процессорах в середине 90-х годов [8]. С момента создания и до сих пор этот режим используется для совершения действий, которые были бы незаметны и практически не отслеживаемы для ОС, но при этом выполняемый код обладал полным доступом к памяти и всем подключенным устройствам [5].

Изначально SMM применялся в области управления питанием компонентов ЭВМ: обработчики событий в SMM собирали статистику по использованию устройств, и, в случае долговременного простоя, устройства отключались [8]. То есть первоначально в задачи SMM не входили какие-либо задачи безопасности, а привилегированный режим был обусловлен необходимостью в постоянном контроле всех устройств ЭВМ. На данный момент задача

управление питанием компонентов ЭВМ не выполняется с помощью SMM, а выполняется при помощи ОС [8].

Для переключения процессора в SMM используются System Management Interruptions (SMIs), которые генерируются компонентами материнской платы, либо могут генерироваться различными драйверами, приложениями (в том числе приложениями из ОС) или пользователями с административными правами в ОС [5]. К типовым системным SMI, которые поддерживаются на данный момент в большинстве ЭВМ (в частности, согласно документации, у компьютеров с 8/9/200/300 сериями чипсетов Intel [9–10, часть 12.8.3.7, 11–12, часть 5.2.4]), можно отнести следующие прерывания и соответствующие им события [5, 9–10, часть 12.8.3.7, 11–12 часть 5.2.4]:

- GPIO Unlock SMI – генерируется при снятии бита Lock (*GLE*) с регистров управления выводами GPIO. Обработчик проверяет ПО, снявшее бит, и если оно не авторизованное, выставляет бит обратно;
- TCO SMI – генерируется при различных событиях. Обработчик прерывания выполняет действия согласно источнику прерывания.
  - Прерывание генерируется Intel TCO watchdog-таймером обратного отсчета при опускании таймера до нуля. Данный таймер должен взводиться ОС каждый несколько секунд. Если таймер опустится до нуля, то будет вызвано прерывание, обработчик которого произведет перезагрузку системы.
  - Прерывание генерируется при выставление бита *BIOSWE* у регистра BIOS Control, отвечающий за возможность читать и писать в флеш-память BIOS'а. Если бит выставляется в SMM, то прерывание не будет сгенерировано, так как выполняемый код уже в SMM режиме; если бит выставляется в любом другом режиме, то прерывание будет сгенерировано, и соответственно будет вызван обработчик, который просто выставит бит обратно. Такой механизм реализован для защиты от перезаписи прошивки ЭВМ из любого режима кроме SMM.
- APMC (APM Control) SMI – генерируется при записи в APM_CNT I/O порт (почти всегда это 0xB2 порт). Срабатывание такого прерывания может быть вызвано администратором ОС при помощи записи в ранее указанный порт. Количество обработчиков может быть 256, при этом при вызове можно указывать номер желаемого обработчика;
- IOTR (IO Trap) SMI – генерируется при обращении к портам CPU I/O. Обработчик позволяют эмулировать Legacy устройства (например, клавиатуру), которые раньше использовали I/O порты;
- xHCI (Extensible Host Controller Interface) SMI – генерируется USB-контроллером при различных событиях.
- Periodic SMI – генерируется чипсетом по таймеру с периодичностью 8/16/32/64 (период настраивается с помощью битов *PER_SMI_SEL*).

1.2. SMM memory (SMRAM). Для изолированности среды выполнения операций в режиме SMM используется память SMM memory (SMRAM), в которой хранятся все необходимые данные для работы SMM: код и обработчики прерываний, а также содержимое регистров (процессор сохраняет контекст при переключение в SMM). Если какая-либо операция выполняется не в режиме SMM, а в обычном режиме (менее привилегированном), то данная память будет недоступна, то есть нельзя как прочитать данные из этого пространства, так и записать в нее что-либо. SMRAM может состоять из следующих областей (вывод об использовании или не использовании сделан по отношению к современным ЭВМ со стандартной конфигурацией SMM) [5,8]:

- ASEG [0x000A0000-0x000BFFFF] – не используется
- HSEG [0xFEDA0000-0xFEDBFFFF] – не используется
- TSEG [настраиваемый диапазон] – используется

1.3. Инициализация SMRAM. Целесообразно рассматривать инициализацию SMRAM и работу SMM с использованием UEFI BIOS, а не Legacy BIOS, так как большинство современных ЭВМ используют именно UEFI интерфейс, а поддержку Legacy BIOS хотят вовсе исключить из современных ЭВМ в ближайшие годы [13].

Весь код SMM (в том числе SMI обработчики) хранится во флеш-памяти UEFI BIOS. Этот код выгружается в SMRAM и конфигурируется однократно при включении ЭВМ на стадии SMM, которая в свою очередь является частью фазы DXE (данные стадии изображены на рисунке 1) [14].

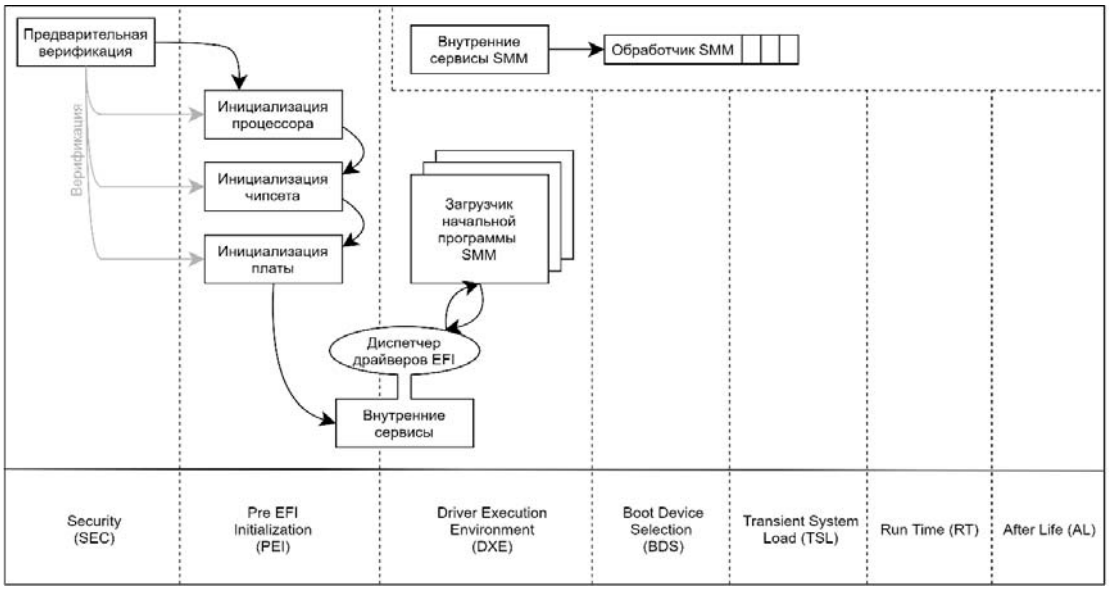


Рис. 1. Фазы загрузки системы с UEFI

После чего данная фаза активна в течение всего временного интервала активности ЭВМ параллельно другим Run Time (RT) фазам.

В процессе инициализация SMRAM выполняется инициализация физической памяти, настройка TSEG, копирование SMM кода в физическую память, настройка таблицы дескрипторов, а также одним из важнейших заключительных этапов является корректное выставление регистров, ответственных за корректную работу памяти и ее защиту.

1.4. Регистры SMM. Для корректной работы SMRAM и настройки доступа к этой памяти используется несколько регистров. Важнейшим и основным регистром является System Management RAM Control (*SMRAMC*) регистр [15, часть 3.29]. Значение *SMRAMC* выставляется при инициализации SMRAM, после чего данный регистр блокируется до следующего рестарта ЭВМ [16]. Среди данных битов регистра наиболее важны биты *D_OPEN* и *D_LCK*, которые должны быть установлены в 0 и 1 соответственно на любой корректно сконфигурированной системе, чтобы SMRAM память была доступна только из кода, выполняемого в SMM.

Также существуют производные регистры для обеспечения корректного доступа к памяти, которые были созданы вследствие обнаружения различных векторов атак на SMM (эти регистры также должны быть корректно сконфигурированы и заблокированы аппаратным обеспечением):

- System Management Range Registers (*SMRR*) – определяет области памяти, в которые запись не из SMM игнорируется, а тип памяти является некешируемым. Должен быть корректно выставлен вендорами. Атака: SMM cache poisoning [17]
- *TSEGMB* регистр у DMA-контроллеров – дублирует информацию о местоположение TSEG, после чего запрещается писать в эту область с помощью DMA. Должен быть корректно выставлен вендорами. Атака: DMA атака [18];
- *SMI_LOCK* бит регистра General PM Configuration, *SMM_BWP* бит регистра BIOS Control – отвечают за генерацию SMI при прошивании BIOS. Атака: отключение генерации SMI, после чего перепрошивка BIOS неавторизованным ПО [19].

2. Функции безопасности с использованием SMM. SMM предназначен для обработки прерываний, которые сгенерированы либо системой (системные SMI), либо прошивкой / драйверами / приложениями, обладающими доступом с правами администратора в ОС

(программные SMI) при помощи записи в *APM_CNT* I/O порт. Таким образом, возможно лишь создание двух типов функции (обработчиков SMI) на основе SMM:

1. Создание обработчика программных SMI. Вызывать такой обработчик можно с помощью ПО в ОС.

2. Расширение обработчика системных SMI. Вызываться такой обработчик будет автоматически при каких-то событиях (зависит от типа SMI).

При этом, учитывая особенности SMM (привилегированность, изолированность среды выполнения кода SMM, хранение кода SMM во флеш-памяти BIOS,), можно говорить о применение обработчиков SMI для создания функций, которым необходимо одно из свойств:

- выполнение привилегированных инструкций;
- выполнение инструкций в изолированной среде по отношению к программной среде в ОС;
- возможность хранения секретных данных малого размера (например, токены, сертификаты, криптографические ключи) в защищенном пространстве, то есть использование части флеш-памяти BIOS как небольшое хранилище данных, к которому можно получить доступ с помощью SMI обработчиков.

В следующих частях рассматриваются более подробно возможные функции безопасности, которые потенциально можно реализовать с помощью обработчиков SMI.

2.1. Создание обработчика программных SMI. Для вызова обработчика программных SMI необходим корректно выставленный бит *APMC_EN* регистра *SMI_EN* [9–10, часть 12.8.3.7, 11–12, часть 5.2.4]. Данный бит является R/W и может быть перезаписан в любой момент, если не реализована соответствующая функциональность блокировки регистра *SMI_EN*. Таким образом, не следует полагаться на гарантированное срабатывание прерывания при отсутствии функциональности блокировки.

Данный обработчик подходит для реализации функций, которые требуется вызывать из ОС для выполнения заведомо определенных привилегированных инструкций. Примеры возможных функций безопасности:

- выполнение мгновенной перезагрузки/выключения системы при выявленных попытках несанкционированного доступа;
- проверка переданных учетных данных и расширение прав доступа пользователя;
- генерация дочерних сертификатов/ключей на основе корневого сертификата/ключа без возможности прочитать корневой сертификат/ключ;
- включение/отключение/проверка компонентов системы и периферийных устройств (например, проверка контрольной суммы флеш-памяти или отключение определенного USB устройства через xHCI интерфейс);
- настройка определенным образом регистров, которые контролируют доступ к компонентам системы и периферийным устройствам (например, включение/выключение возможности записи на жесткий диск).

2.2. Расширение обработчика системных SMI. Для вызова обработчика системных SMI необходим корректно выставленный бит включения прерываний для соответствующего типа прерываний регистра *SMI_EN* [9–10, часть 12.8.3.7, 11–12, часть 5.2.4]. Большинство таких битов являются R/W и могут быть перезаписаны в любой момент, если не реализована соответствующая функциональность блокировки регистра *SMI_EN*. Таким образом, не следует полагаться на гарантированное срабатывание прерывания при отсутствии функциональности блокировки. Но для некоторых прерываний предусмотрена встроенная функциональность блокировки соответствующего бита, так, например, для всех современных ЭВМ x86 архитектуры такими битами являются: *GPIO_UNLOCK_SMI_EN* и *TCO_EN*.

На базе таких обработчиков можно реализовать более специфичные функции с автоматически генерируемыми прерываниями различными компонентами системы при соблюдение определенных условий (зависит от компонента и типа SMI). Примеры возможных функций безопасности:

- обработчик TCO SMI можно модифицировать для обработки запросов на перезапись прошивки;

● обработчик GPIO Unlock SMI можно модифицировать, либо вовсе заменить своим обработчиком для контроля доступа ОС к определенным GPIO-контактам;

● обработчик xHCI SMI (*xHCI_SMI_EN* бит является R/W) можно модифицировать, либо дополнить необходимыми функциями, чтобы обрабатывать различные события, связанные с USB устройствами [20 часть 4.22.1];

● обработчик Periodic SMI (*PERIODIC_EN* бит является R/W) можно модифицировать, либо дополнить необходимыми функциями, чтобы выполнять определенный код многократно с определенным периодом.

3. Плюсы и минусы SMM для СЗИ. Плюсы и минусы разделены на фундаментальные и технические, где первые особо важны, так как они являются архитектурной особенностью режима, а, следовательно, они никаким образом не могут быть значительно изменены в последующих обновлениях прошивки в отличие от технических атрибутов SMM.

3.1. Плюсы SMM

3.1.1 Фундаментальные

1) *Привилегированный доступ.* В базовом сценарии, SMM предоставляет максимальный доступ к системе среди прочих встроенных в систему технологий (за исключением технологий, которые базируются на РКБ).

2) *Дешевизна и высокая бесперебойность.* Решение на базе SMM не нуждается в дополнительном аппаратном оборудовании, а реализуются уже в существующем окружении, что положительно сказывается на бесперебойности СЗИ и количестве возможных аппаратных неисправностей, а также на стоимости самого решения.

3.1.2 Технические

3) *Ранняя стадия старта функционирования.* SMM код загружается и запускается в DXE фазе загрузки UEFI. Это фаза идет после фаз SEC и PEI, и до фазы Boot Device Selection (BDS) (см. рис. 1) [21]. И с одной стороны, наличие двух фаз перед запуском SMM является, определенно, минусом, но с другой стороны это позволяет коду SMM работать с памятью (которая инициализируется в PEI) и работать с устройствами системы. При этом полноценно функционировать SMM начинает после блокирования SMRAM, до окончания фазы DXE, т. е. в конце фазы DXE SMRAM уже находится в заблокированном состояние, и SMM может обрабатывать приходящие запросы. Поэтому в фазе BDS можно говорить о полном функционировании данной технологии.

4) *Встроенная защита кода SMM от перезаписи.* Одной из основных задач SMM на данный момент является обработка запросов системы на прошивание флеш-памяти BIOS, где и хранится код SMM. Таким образом, при правильной конфигурации SMM можно защитить SMM код от несанкционированных воздействий (не рассматривается прошивание памяти с помощью аппаратного воздействия).

3.2. Минусы SMM

3.2.1. Фундаментальные

1) *Доверие к вендору.* При использовании SMM необходим РКБ для построения доверенной системы (в том числе для того, чтобы контролировать недоверенный процессор [22]), либо необходимо доверять процессору, который в таком случае возьмет на себя задачи по выполнению отдельных задач РКБ, и, соответственно, доверять вендору. Также, поскольку системные SMI генерируется различными компонентами системы (например, xHCI контроллером, отвечающий за взаимодействие с USB), необходимо доверять этим контроллерам в части срабатывания прерываний на определенные события или действия.

3.2.2. Технические

2) *Платформозависимость.* Данная технология сильно платформозависима (и разработана только для x86 архитектуры) по своей реализации и написанию драйверов для SMM. Также не менее важным является факт, что вендоры (в том числе Intel, AMD) не гарантируют наличие тех или иных системных SMI в системе по умолчанию (это можно проследить в документации [9–10, часть 12.8.3.7; 11–12, часть 5.2.4]).

3) *Ограничения по памяти.* Согласное документации под сегмент TSEG SMRAM может быть выделено 1, 2 или 8 MB (мегабайт) [16, часть 3.37], что ставит ограничения на разрабатываемый код.

4) *Большинство битов в регистре SMI_EN являются R/W.* Так как большинство битов в данном регистре является R/W, то нельзя полагаться на срабатывание конкретных SMI. Либо необходимо разработать собственную логику в SMM, которая сможет блокировать необходимый бит.

3.3. Возможные СЗИ. Таким образом, наиболее целесообразным и простым использованием SMM является применение этой технологии для реализации небольшого хранилища данных, либо функций, к которым будет ограничен доступ на чтение и изменение посредством SMI обработчиков. При этом обеспечить взаимодействие с этой частью памяти и получать доступ к ней можно напрямую из ОС. Примеров реализации коммуникации кода ОС и SMM кода на данный момент достаточно [14, 23, 24].

С другой стороны, можно использовать автоматически генерируемые SMI, создаваемые Platform Controller Hub'ом (PCH) при определенных событиях. Но данный способ является эффективным только в случае блокировки битов, отвечающих за срабатывание прерываний, поэтому необходимо также реализовать дополнительную функциональность, которая будет отвечать за неизменность этих битов. Документация Intel не декларирует возможностей по блокировке таких битов [9–10, часть 12.8.3.7, 11–12 часть 5.2.4], а примеры атак [25] на изменение таких битов еще раз подтверждают наличие векторов атак в случае реализации СЗИ через SMI. Однако существует патент по реализации блокировки регистра *SMI_EN* (см. [26]), но он скорее декларирует и описывает архитектурную возможность по аппаратному улучшению чипсета (в частности, южного моста чипсета), нежели возможность по реализации блокировки регистра с помощью программных средств. Таким образом, предлагаемый вариант блокировки в патенте может быть целесообразен для вендоров компьютерной техники, поскольку они могут вносить существенные изменения в структуру элементов ЭВМ, но не является целесообразным для разработчиков СЗИ.

Заключение. Как итог, поскольку выполняемый в SMM код обладает достаточно привилегированным доступом в ЭВМ, этот режим остается крайне интересен для исследования на уязвимости с целью выработки рекомендаций по корректному конфигурированию. При этом из-за архитектурных особенностей данной технологии, реализация каких-либо новых инструментов безопасности с использованием SMM представляет собой сложную (нецелесообразную) задачу. Поэтому в современных ЭВМ необходимо правильно конфигурировать SMM, и не следует полагаться на данную технологию при разработке СЗИ.

Список литературы

1. Domas, C. The Memory Sinkhole / C. Domas // Официальный сайт конференции Black Hat [Электронный ресурс]. – Режим доступа : https://www.blackhat.com/docs/us-15/materials/us-15-Domas-The-Memory-Sinkhole-Unleashing-An-x86-Design- Flaw- Allowing- Universal-Privilege-Escalation-wp.pdf. – Дата обращения : 14.11.2020.

2. Oster, J. E. Getting Started with Intel® Active Management Technology (Intel® AMT) [Электронный ресурс] / J. E. Oster // Официальный сайт компании Intel. – Режим работы : https://software.intel.com/ content/www/us/en/develop/ articles/getting-started-with-intel-active-management-technology-amt.html (дата обращения: 18.11.2020).

3. О безопасности UEFI, часть заключительная [Электронный ресурс]. – Режим работы : https://habr.com/ru/post/268423/. – Дата обращения : 18.11.2020.

4. Jiewen, Y. A Tour Beyond BIOS Launching STM to Monitor SMM in EDK II [Электронный ресурс] / Y. Jiewen, J. V. Zimmer // Официальный сайт компании Intel. – Режим доступа : https://software.intel.com/content/dam/develop/external/us/en/documents/a-tour-beyond-bios-launching-stm-to-monitor-smm-in-efi-developer-kit-ii-819978.pdf. – Дата обращения : 18.11.2020.

5. О безопасности UEFI, часть вторая [Электронный ресурс]. – Режим доступа : https://habr.com/ru/post/267197/. – Дата обращения : 18.11.2020.

6. Rauchberger, J. LONGKIT – A Universal Framework for BIOS/UEFI Rootkits in System Management Mode / J. Rauchberger, R. Luh, S. Schrittwieser // Conference: 3rd International Conference on Information Systems Security and Privacy. – P. 346–353.

7. Банк данных угроз безопасности информации. SMM [Электронный ресурс] // Официальный сайт ФСТЭК. – Режим доступа : https://bdu.fstec.ru/search?q=SMM. – Дата доступа : 18.11.2020.

8. SMM и SMRAM или 128 Кб потусторонней памяти: исследовательская работа №5 [Электронный ресурс]. – Режим доступа : https://xakep.ru/2008/07/29/44663/. – Дата доступа : 18.11.2020.

9. Intel® 8 Series/C220 Series Chipset Family Platform Controller Hub (PCH) [Электронный ресурс] // Официальный сайт компании Intel. – Режим доступа : https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/8-series-chipset-pch-datasheet.pdf. – Дата доступа : 18.11.2020.

10. Intel® 9 Series Chipset Family Platform Controller Hub (PCH) // Официальный сайт компании Intel [Электронный ресурс]. – Режим доступа : https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/9-series-chipset-pch-datasheet.pdf. – Дата доступа : 18.11.2020.

11. Intel® 200 (Including X299) and Intel® Z370 Series Chipset Families Platform Controller Hub (PCH). Volume 2 [Электронный ресурс] // Официальный сайт компании Intel. – Режим доступа : https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/200-series-chipset-pch-datasheet-vol-2.pdf. – Дата доступа : 18.11.2020.

12. Intel® 300 Series and Intel® C240 Series Chipset Families Platform Controller Hub (PCH). Volume 2 [Электронный ресурс] // Официальный сайт компании Intel. – Режим доступа : https://www.intel.com/ content/dam/www/public/us/en/documents/datasheets/300-series-chipset-pch-datasheet-vol-2.pdf. – Дата доступа : 18.11.2020.

13. Intel to Remove Legacy BIOS Support from UEFI by 2020 [Электронный ресурс]. – Режим доступа : https://www.anandtech.com/show/12068/intel-to-remove-bios-support-from-uefi-by-2020. – Дата доступа : 09.05.2021.

14. Building reliable SMM backdoor for UEFI based platforms [Электронный ресурс]. – Режим доступа : http://blog.cr4.sh/2015/07/building-reliable-smm-backdoor-for-uefi.html. – Дата доступа : 18.11.2020.

15. 8th and 9th Generation Intel® Core™ Processor Families and Intel® Xeon ^{E} Processor Family // Официальный сайт компании Intel [Электронный ресурс]. – Режим доступа : https://www.intel.com/content/dam/www/public/us/en/ documents/datasheets/8th-gen-core-family-datasheet-vol-2.pdf. – Дата доступа : 18.11.2020.

16. Intel® Platform Innovation Framework for EFI System Management Mode Core Interface Specification (SMM CIS) [Электронный ресурс] // Официальный сайт компании Intel. – Режим доступа : IItps://www.intel.ru/content/dam/ doc/reference-guide/efi-smm-cis-v091.pdf. – Дата доступа : 18.11.2020.

17. Attacking SMM Memory via Intel® CPU Cache Poisoning [Электронный ресурс]. – Режим доступа : https://invisiblethingslab.com/resources/misc09/smm_cache_fun.pdf. – Дата доступа : 18.11.2020.

18. Attacking UEFI Boot Script [Электронный ресурс]. – Режим доступа : https://bromiumlabs.files. wordpress. com/2015/01/venamis_whitepaper.pdf (дата обращения: 18.11.2020).

19. О безопасности UEFI, части нулевая и первая [Электронный ресурс]. – Режим доступа : https://habr.com/ ru/post/266935/. – Дата доступа : 18.11.2020.

20. eXtensible Host Controller Interface for Universal Serial Bus (xHCI) // Официальный сайт компании Intel [Электронный ресурс]. – Режим доступа : https://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/extensible-host-controler-interface-usb-xhci.pdf. – Дата обращения : 18.11.2020.

21. Устройство файла UEFI BIOS, часть полуторная: UEFI Platform Initialization [Электронный ресурс]. – Режим доступа : https://habr.com/ru/post/185764/. – Дата доступа : 18.11.2020.

22. Елькин, В. М. Контроль недоверенного процессора / В. М. Елькин // Комплексная защита информации: материалы XXIII науч.-практ. конф., Суздаль, 22–24 мая 2018 г. – М. : Медиа Групп «Авангард», 2018. – С. 209–211.

23. System Management Mode Hacks [Электронный ресурс]. – Режим доступа : http://phrack.org/issues/65/7.html. – Дата обращения : 18.11.2020.

24. Использование Intel Processor Trace для трассировки кода System Management Mode [Электронный ресурс]. – Режим доступа : https://habr.com/ru/company/dsec/blog/481692/. – Дата обращения : 18.11.2020.

25. Advanced x86: Introduction to BIOS & SMM. SMI Suppression [Электронный ресурс]. – Режим доступа : https://opensecuritytraining.info/IntroBIOS.html. – Дата обращения : 18.11.2020.

26. Ziarnik G. P., Durham M. R., Piwonka M. A. Pattern № US9483426B2, United States (US). Locking a system management interrupt (SMI) enable register of a chipset. Appl. № US14/364,706; PCT Filed 31.01.2012; PCT № PCT/US2012/023225; PCT Date 12.06.2014; Publication Date 01.11.2016. Assignee: Hewlett-Packard Development Company, L.P.

УДК 004

РАЗРАБОТКА СИСТЕМЫ СИНТЕЗА РЕЧЕПОДОБНОГО СИГНАЛА

К.П. ШАКИН
Научно-производственное унитарное предприятие
«Научно-исследовательский институт технической защиты информации»
г. Минск, Республика Беларусь

Введение. Защита акустической речевой информации является одной из важнейших задач по обеспечению информационной безопасности и осуществляется с использованием пассивных и активных методов защиты информации.

Пассивные методы защиты информации предполагают ослабление непосредственно акустических сигналов, циркулирующих в помещении, а также продуктов электроакустических преобразований в соединительных линиях ВТСС, возникающих как естественным путем, так и в результате ВЧ навязывания.

Активные методы защиты акустической речевой информации предполагают создание вибрационных и акустических маскирующих шумовых помех средствам акустической речевой разведки. Для этих целей используются системы виброакустической маскировки, включающие генераторы белого и розового шума. В последнее время большой интерес стала вызывать речеподобная помеха, которая по своему спектральному составу близка к речевому сигналу.

Для реализации устройства защиты речевой информации, генерирующего речеподобную помеху, предлагается применить систему синтеза речеподобных сигналов на основе компиляционного метода, основная идея которого заключается в соединении готовых минимальных акустических единиц. При использовании этой модели составляется база данных звуковых фрагментов, из которых в дальнейшем будет синтезироваться речь. Размер элементов синтеза, как правило, не меньше слова.

1. Оценка эффективности защиты информации. Особенностью акустической речевой разведки является то, что анализ перехваченной информации производит человек. Поэтому в качестве показателя речевой информации используется словесная разборчивость речи Wc, под которой понимается относительное количество (в процентах) правильно понятых слов из перехваченного средством разведки разговора.

Словесная разборчивость речи отражает качественную область понятности, которая выражена в категориях подробности составляемой справки о перехваченном с помощью технических средств разведки разговоре.

Для оценки разборчивости речи наиболее часто используется инструментально-расчетный метод.

Спектр речи разбивается на 7 октавных полос со среднегеометрическими частотами: 125; 250; 500; 1000; 2000; 4000 и 8000 Гц.

Для каждой октавной частотной полосы экспериментально определяются формантный параметр ΔA_i, дБ, характеризующий энергетическую избыточность дискретной составляющей речевого сигнала, а также весовой коэффициент k_i, характеризующий вероятность наличия формант речи в данной октавной полосе частот.

Характеристики октавных полос речевого диапазона и экспериментально определенные значения формантного параметра спектра речевого сигнала ΔA_i и весовых коэффициентов k_i для октавных полос представлены в таблице 1.

Для каждой i-й октавной полосы измеряется или рассчитывается отношение «уровень речевого сигнала/уровень шума» q_i, дБ. На основе q_i рассчитывается коэффициент восприятия формант слуховым аппаратом человека p_i, представляющий собой вероятное относительное количество формантных составляющих речи, которые будут иметь уровни интенсивности выше порогового значения восприятия.

Таблица 1

Характеристики октавных полос частотного диапазона речи

Номер полосы	Частотные границы полосы *f*н-*f*в, Гц	Средняя геометрическая частота полосы *fi*, Гц	Весовой коэффициент полосы *ki*	Значение формантного параметра речи в полосе Δ*ai*, дб
1	90–175	125	0,01	25
2	175–355	250	0,03	18
3	355–710	500	0,12	14
4	710–1400	1000	0,2	9
5	1400–2800	2000	0,3	6
6	2800–5600	4000	0,26	5
7	5600–11200	8000	0,07	4

$$p_i = \begin{cases} \dfrac{0{,}78 + 5{,}46 \cdot \exp\cdot\left[-4{,}3 \cdot 10^{-3} \cdot \left(27{,}3 - |Q_i|\right)^2\right]}{1 + 10^{0.1 \cdot |Q_i|}}, \\ 1 - \dfrac{0{,}78 + 5{,}46 \cdot \exp\cdot\left[-4{,}3 \cdot 10^{-3} \cdot \left(27{,}3 - |Q_i|\right)^2\right]}{1 + 10^{0.1 \cdot |Q_i|}}; \\ \text{если } Q_i > 0 \end{cases}$$

$$Q_i = q_i - \Delta A_i,$$

Далее рассчитывается спектральный индекс артикуляции (понимаемости) речи R_i и интегральный индекс артикуляции речи R.

$$R_i = p_i \cdot k_i.$$

$$R = \sum_{i=1}^{i=7} R_i.$$

Словесная разборчивость речи W связана с интегральным индексом артикуляции речи соотношением

$$W = \begin{cases} 1{,}54 \cdot R^{0{,}25} \cdot \left[1 - \exp(-11 \cdot R)\right] \\ R < 0{,}15 \\ 1 - \exp\left(-\dfrac{11 \cdot R}{1 + 0.7 \cdot R}\right). \\ R \geq 0{,}15 \end{cases}$$

Критерии эффективности защиты речевой информации во многом зависят от целей защиты: скрыть смысловое содержание ведущегося разговора, скрыть тематику ведущегося разговора или скрыть сам факт ведения переговоров.

Как показывает практика, составление подробной справки о содержании перехваченного разговора невозможно при словесной разборчивости менее 70–80 %, а краткой справки – при словесной разборчивости менее 40–60 %. При словесной разборчивости менее 20–40 % значительно затруднено установление даже предмета ведущегося разговора, при словесной разборчивости менее 10–20 % – это практически невозможно.

2. Система синтеза речеподобных сигналов для защиты информации. Предлагаемая система синтеза речеподобных сигналов включает в себя следующие функции:

- анализ и обработка входного текста;
- формирование фонем и аллофонов;
- компиляция и генерация речевого сигнала;

В целях реализации системы синтеза речеподобных сигналов разработан программ-

ный модуль синтеза речеподобных сигналов, который предполагает формирование фонемного текста и компиляцию баз аллофонов. В качестве минимальной акустической единицы используется аллофон. Структура программного модуля включает:

– генератор псевдотекста;

– база аллофонов;

– компиляционный синтезатор речи;

– акустическая система

В качестве основы компиляционного синтезатора речи целесообразно использовать два больших блока: обработки естественного языка и обработки цифрового сигнала.

1. Модуль обработки естественного языка выполняет анализ и обработку входного орфографического текста. Непосредственно в прикладных системах модуль естественного языка делится на три подмодуля: лингвистической, фонетической и просодической обработки.

В подмодуль лингвистической обработки включены такие функции, как очистка текста, расшифровка числительных, даты и времени, аббревиатур, сокращений, Интернет ресурсов, автоматическая расстановка ударений, объединение слов в акцентные группы и членение на синтагмы.

В подмодуле фонетической обработки выполняется автоматическое транскрибирование текста в фонемный вид, а затем фонемного текста в аллофонный.

При этом ударные гласные маркируются индексом 0, предударные индексом 1, заударные индексом 2. В служебных словах ударная гласная маркируется индексом 5, а порядок индексирования заударных и предударных при их наличии остается прежний.

Просодическое оформление текстовой информации, в лингвистической обработке, заключается в сопоставлении интонационных контуров к соответствующим типам синтагм. Для этого необходимо классифицировать акцентные группы и разделить их на составляющие.

2. Модуль обработки цифрового сигнала заключается лишь в акустическом подмодуле. Основная задача акустического модуля – генерация (синтез) речевого сигнала на основе трех типов параметров:

– просодических параметров (F0 – частота основного тона, T – длительность звуков, a – амплитуда звуков), которые поступают от просодического подмодуля;

– фонетических параметров, поступающих от фонетического подмодуля (в зависимости от типа фонетического процессора эти параметры могут быть различными: формантными параметрами ($F1$, $F2$, $A1$...), параметры сечений речевого тракта, номер аллофона или сегмента и т. д.);

– параметры синтезируемого голоса, обеспечивающие желаемую тембровую индивидуальность.

В результате на выходе компиляционного синтезатора речи формируется речеподобная помеха, которая в дальнейшем поступает на вход акустической системы.

Заключение. Предлагаемая система синтеза речеподобных сигналов обеспечивает защиту информации с помощью заранее сформированных баз аллофонов, однако ее можно адаптировать и к формированию баз аллофонов из речи диктора в режиме реального времени.

Стоит отметить, что данный способ обеспечивает высокое качество синтезируемой речи, т. к. позволяет воспроизводить форму естественного речевого сигнала. Еще одно достоинство данного подхода: не требуется никаких знаний об устройстве речевого тракта и структуре языка.

Список литературы

1. Хорев, А.А. Способы защиты выделенных помещений от утечки речевой (акустической) информации по техническим каналам: системы виброакустической защиты / А. А. Хорев // Специальная техника. – 2013. – № 4. – С. 31–63.

2. Фролов, А. Синтез и распознавание речи / А. Фролов, Г. Фролов. – М., 2008.

3. Рыбин, С. В. Синтез речи / С. В. Рыбин. – СПб. : Университет ИТМО, 2014.

4. Киселев, В. В. Доклады БГУИР / В. В. Киселев, Б. М. Лобанов. – Минск, 2004.

5. Бузов, Г.А. Защита от утечки информации по техническим каналам : учеб. пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М. : Горячая линия – Телеком, 2005.

УДК 004.056.2

КОНТРОЛЬ ЦЕЛОСТНОСТИ ВИРТУАЛЬНЫХ МАШИН НА ПЛАТФОРМЕ OPENSTACK

Д.О. СТАСЬЕВ
Федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (национальный исследовательский университет)», г. Долгопрудный, Российская Федерация

Введение. Согласно аналитическому исследованию [1], проведенному компанией «Код Безопасности» в 2018 году среди 305 участников (IT-директора, ведущие инженеры, специалисты по защите информации, руководители направлений информационной безопасности), значительная часть организаций, независимо от масштабов их бизнеса, используют виртуализацию в серверной инфраструктуре более чем на 50% серверов. Применение данной технологии позволяет эффективно использовать вычислительные мощности оборудования, сокращает время его простоя, однако создает опасность – появляется дополнительный канал для проникновения злоумышленника, повышается вероятность потери конфиденциальных данных, обрабатываемых на серверах с виртуализацией 70% российских компаний-респондентов. Поэтому несмотря на то, что в среднем только 38% российских компаний опасаются действий злоумышленника, актуальность рассмотрения вопросов обеспечения безопасности при использовании виртуализации остается высокой.

Например, OpenStack, являясь одной из популярных платформ для создания виртуальных инфраструктур (ВИ – это система, которая обеспечивает поддержку виртуализации серверов, сети и хранилищ данных, создается с помощью инфраструктуры виртуализации), не предоставляет надежных механизмов контроля целостности (КЦ) ВИ и создаваемых в ней виртуальных машин (ВМ). Только в 2015 году в OpenStack начали внедрять защитные функции, такие как, например, КЦ образов ВМ [2]. Для его реализации изначально стали использовать подпись (RSA-PSS) контрольной суммы, вычисленной от данных образа ВМ с помощью алгоритма хеширования MD5, который не является криптографически стойким. Отсутствие криптостойкости позволяло злоумышленнику заменить исходный образ ВМ на произвольный (злоумышленник мог добиться коллизии между значениями хеш-функции от исходного образа и произвольного). В 2016 году от контрольной суммы отказались, заменили ее вычислением подписи от содержимого образа напрямую [3]. Однако несмотря на это, в OpenStack оставались критические уязвимости. Например, в случае несовпадения хранимой и заново вычисленной подписей, платформа выводила сообщение (в логах ошибок) о невозможности создания ВМ, содержащее требуемое значение подписи. Злоумышленник, получив информацию о требуемом для создания образа значении подписи, получал возможность так заменить значение подписи для своего образа в базе данных (БД), что создание ВМ из его образа не блокировалось системой. Иными словами, злоумышленник получил возможность создавать ВМ из произвольного образа, потенциально содержащего программные закладки или любое другое вредоносное программное обеспечение [4].

Несмотря на активное развитие OpenStack и исправление ошибок, в настоящее время в платформе продолжают находить уязвимости, которые создают угрозы различных уровней [5]. Таким образом, кроме использования встроенных в OpenStack механизмов защиты от злоумышленников необходимо использовать дополнительные наложенные средства защиты информации (СЗИ).

При создании СЗИ для КЦ ВМ в OpenStack-based ВИ необходимо реализовывать не только мониторинг целостности критических файлов самих ВМ, но и метаданных образов ВМ (хранятся в отдельной БД в OpenStack). В свою очередь, только КЦ ВМ и образов ВМ недостаточно для осуществления полноценного КЦ всей OpenStack-based ВИ. Необходимо дополнительно обеспечивать КЦ конфигурации (связи в графе конфигурации ВИ [6]) и компонентов ВИ [7]. Получаем, что КЦ OpenStack-based ВИ – комплексная задача, для ре-

шения которой необходим мониторинг целостности как отдельных компонентов ВИ, так и связей между ними.

Данная статья посвящена решению одной из частей описанной задачи КЦ ВМ в OpenStack – КЦ конфигураций образов ВМ.

1. Компоненты OpenStack, участвующие во взаимодействии с ВМ. Перед исследованием особенностей платформы OpenStack введем основные понятия в области серверной виртуализации. Гипервизор – программа и/или аппаратная система, обеспечивающая одновременное, параллельное выполнение нескольких сред (каждая среда обычно является программной системой, содержит операционную систему (ОС) и эмулирует аппаратное обеспечение некоторой target-платформы) на одном хост-компьютере (host-платформе). Экземпляром ВМ (или просто ВМ) будем называть отдельную среду, которую можно получить с помощью гипервизора. Образом ВМ именуем совокупность файлов (может состоять из одного), используемую в качестве шаблона (образца) при создании новых экземпляров ВМ.

OpenStack – это система, состоящая из комплекса программного обеспечения (ПО), созданная для управления большими наборами вычислительных ресурсов, хранилищ и сетевых ресурсов [8]. Платформа OpenStack предоставляет архитекторам ВИ набор компонентов (сервисов), с помощью которых можно разработать архитектуру и создать требуемую ВИ, управлять как состоянием ВМ, так и аппаратными ресурсами.

Можно выделить несколько сервисов, которые созданы в OpenStack для взаимодействия с ВМ. OpenStack Glance используется для управления образами (шаблонами) ВМ (например, для добавления и удаления образов). Созданием ВМ из образов занимается сервис OpenStack Nova (рис. 1). При создании ВМ Nova обращается к Glance, который получает образ из какого-либо хранилища. Сервис Nova кроме создания экземпляров ВМ позволяет ими управлять [9], например, можно менять аппаратные ресурсы ВМ с помощью применения (смены) готовых конфигураций (содержат размер доступной оперативной и постоянной памяти экземпляру ВМ), называемых flavor. Также Nova позволяет выбрать и настроить гипервизоры для ВМ. Сами файлы образов и экземпляров ВМ находятся в отдельном хранилище. В зависимости от конфигурации OpenStack-based ВИ тип и реализация хранилища могут быть разными: в самом простом случае им может быть файловая система хост-компьютера, однако на практике часто используют специальные сервисы OpenStack, реализующие хранилища (OpenStack Swift, OpenStack Cinder) [10–11]. Для аутентификации и авторизации пользователей в OpenStack используется сервис Keystone. Под пользователями в нем понимают, как людей, работающих непосредственно с ВИ (например, администраторов и архитекторов ВИ), так и сервисы OpenStack, между которыми происходит взаимодействие. Рассматриваемые сервисы OpenStack (Glance, Nova, Keystone) реализованы как один, либо как набор web-серверов, поэтому взаимодействие с ними и между ними происходит с помощью HTTP запросов с соответствующими заголовками (для Keystone).

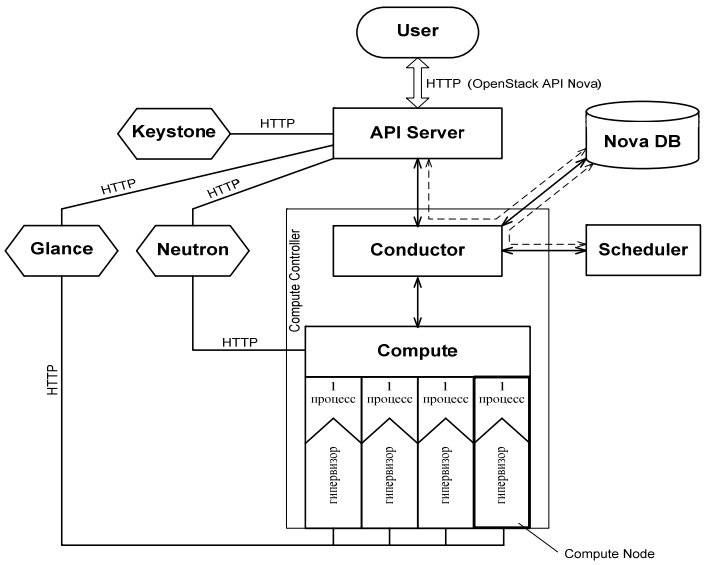


Рис. 1. Схема взаимодействия частей OpenStack Nova

2. Хранение образов ВМ и их конфигураций в OpenStack. Жизненным циклом ВМ будем называть совокупность процессов и состояний системы, связанных с созданием, использованием, хранением и удалением экземпляров ВМ. Для обеспечения целостности ВМ необходим КЦ на всех этапах жизненного цикла ВМ. Первым этапом жизненного цикла ВМ является ее создание из образа ВМ.

OpenStack предоставляет широкие возможности по взаимодействию с образами ВМ с помощью сервиса Glance, рассмотрим его подробнее. Glance (Image service) – компонент, созданный для управления образами ВМ и метаданными ВИ [12–13]. Под метаданными понимают элементы ассоциативного массива (пары «ключ-значение»), которыми могут управлять администраторы ВИ (например, могут создавать, удалять, применять к образам ВМ). До применения метаданных к конкретным ресурсам OpenStack они не влияют на ВИ, но после добавления метаданных к различным объектам OpenStack, объекты могут использовать метаданные как источник настроек, то есть метаданные могут влиять на конфигурацию частей ВИ.

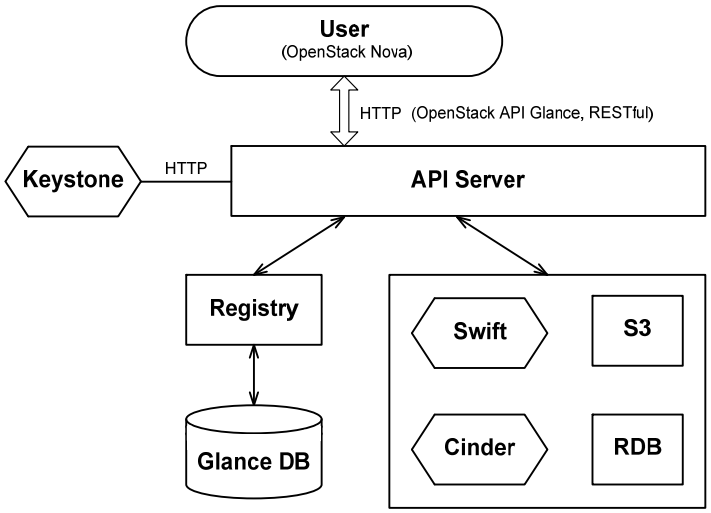


Рис. 2. Схема взаимодействия частей OpenStack Glance

Сервис Glance состоит большого числа внутренних подсистем [14]. С помощью применения метода абстрагирования можно выделить четыре основные части, представлены на рисунке 2: Glance API Server, Glance Registry, Glance DB (каталог метаданных) и хранилище образов и файлов ВМ. Glance Registry является основной частью Glance, предоставляет Glance API Server информацию о наличии образов в Glance и об их расположении в хранилище с помощью Glance DB. Glance DB является БД, которая содержит метаданные и расположение каждого образа в хранилище. Обычно для Glance DB используют реляционную БД, созданную на основе таких систем управления БД (СУБД), как MySQL и SQLite (являются наиболее популярными СУБД для OpenStack) [13–15]. Часто СУБД для Glance DB является единственной во всей OpenStack-based ВИ, поэтому она может использоваться и другими сервисами (обычно создается новый пользователь СУБД для отдельной требуемой БД для каждого сервиса, например, такой механизм реализован в OpenStack Nova). Образы ВМ, доступные через Glance, могут храниться в самых разных местах, от простых файловых систем до систем хранения, таких как проекты OpenStack Swift, OpenStack Cinder или S3 [12]. Для работы Glance необходим Keystone.

3. Glance DB и эталон конфигурации образа ВМ. Так как для КЦ ВИ необходим, в частности, КЦ образов ВМ и их конфигураций, хранимых в Glance DB, то для КЦ самих образов, находящихся в хранилище, требуется вычислять контрольные суммы от содержимого файлов. Перейдем к исследованию Glance DB, где хранятся метаданные и свойства образов ВМ. Можно объединить таблицы в несколько групп в соответствии с их ролями во взаимодействии с образами ВМ (табл. 1).

После определения ролей таблиц БД glance во взаимодействии с образами ВМ можно перейти к вопросам КЦ образов ВМ. КЦ предполагает сравнение текущего состояния системы с некоторым его выбранным, фиксированным состоянием, принятым за эталон [18]. После задания эталона в определенные моменты времени происходит сравнение актуального состояния системы с записанным в эталон. Наличие таких механизмов позволяет контролировать целостность системы [19]. В случае КЦ образов и метаданных образов ВМ в эталон образа ВМ должны входить поля таблиц (3) – (7), для КЦ метаданных всей ВИ необходимы таблицы (10) – (15).

Поскольку рассматривается разработка механизма КЦ конфигураций образов ВМ, то эталон конфигураций образов ВМ должен включать поля таблиц (3) – (7). Для вычисления значения эталона в данной работе будут использоваться: идентификатор образа ВМ (GUID,

Globally Unique Identifier) (поле id таблицы images (7) БД glance) и значение хеш-функции (контрольная сумма) от значений таблиц (3) – (7). В будущем предполагается, что данные пары будут храниться в аппаратно-защищенной области постоянной памяти. Для дополнительной защиты можно использовать идею патента [20] после согласования с патентообладателем: вычислять контрольную сумму не только от хранимых данных, но и от контрольной суммы предыдущей записи и ключа хранения, используемого программным модулем для подписи записываемых значений. Согласно патенту, можно использовать криптографию с открытым ключом, в которой подписывающее лицо (программный модуль) вычисляет контрольную сумму проверки целостности с помощью своего закрытого ключа, а лицо, желающее проверить целостность, может использовать свой открытый ключ для верификации. Вычисленная контрольная сумма присоединяется к записи данных [20].

Таблица 1

Связь таблиц БД glance и их ролей во взаимодействии с образами ВМ

Роль во взаимодействии с образами ВМ	Таблицы
Используются для миграций (SQLAlchemy)	1. alembic_version 2. migrate_version
Содержат информацию о хранимых образах ВМ	3. image_locations 4. image_members 5. image_properties 6. image_tags 7. images
Используются для обработки “больших“ образов ВМ сервисом Glance [16]	8. task_info 9. tasks
Необходимы для хранения метаданных [17]	10. metadef_properties 11. metadef_tags 12. metadef_resourse_types 13. metadef_objects 14. metadef_namespaces 15. metadef_namespace_resource_types

Таким образом, поскольку разрабатывается механизм КЦ конфигураций образов ВМ, то эталон образа ВМ должен включать значения таблиц (3) – (7) БД glance.

4. Взаимодействие разрабатываемого программного модуля с эталонами конфигурации образов ВМ, внедрение СЗИ в OpenStack. Опишем предполагаемую архитектуру разрабатываемого программного модуля. Ее функционирование будет основано на вычислении эталона образа ВМ и его хранении в памяти хост-компьютера. В некоторые моменты времени функция в разрабатываемом модуле для создания эталона будет заново вычисляться и полученное значение будет сравниваться с записанным в память эталоном. В случае несовпадения вычисленного значения и эталона, администратор ВИ будет получать уведомление о нарушении КЦ конфигураций образов ВМ. Система должна запрещать создание ВМ из образов при нарушении КЦ конфигураций образов, при своих ошибках, например, при отсутствии возможности получения данных из БД для вычисления образа.

Модуль должен запускаться до старта ВИ, чтобы создавать эталоны для всех добавляемых образов ВМ в ВИ. Определим в какие моменты времени (в ответ на какие события) система должна вычислять эталоны. Изначально при добавлении образа ВМ в ВИ необходимо создавать исходные эталоны и помещать их в файл (возможно применение аппаратно-защищенной области памяти для хранения файла). При попытке создания экземпляра ВМ из образа ВМ должен заново вычисляться эталон и сравниваться с записанным в файл. Дополнительно образ используется при запуске созданной ВМ.

Определим, как отслеживать необходимые для КЦ конфигураций образов ВМ события (добавление образа ВМ в ВИ, создание экземпляра ВМ из образа и запуск ВМ) в платформе OpenStack. Есть несколько решений. Старт ВМ и ее создание из образа происходит с помощью обработки соответствующих запросов сервисом OpenStack Nova. Посколь-

ку Nova является совокупностью нескольких сервисов, общающихся с помощью очереди сообщений RabbitMQ, то можно читать эти сообщения (то есть можно встроить модуль в сам сервис Nova). Однако формат этих сообщений строго не определен (поскольку является внутренней служебной частью сервиса), и поэтому существует риск возникновения проблем с совместимостью разрабатываемого СЗИ с новыми версиями платформы OpenStack. Поскольку OpenStack активно развивается и выпускает несколько релизов в год, то потенциальные затраты на поддержание работоспособности такого СЗИ высоки. Кроме того, очередь сообщений обрабатывает большое число запросов между внутренними сервисами OpenStack Nova, поэтому система для их чтения будет требовать значительных ресурсов.

Другим решением может стать создание прокси-сервера для обработки запросов к OpenStack Nova. Упрощенно Nova API Server (часть OpenStack Nova, рисунок 1) можно считать HTTP сервером. Взаимодействие между пользователем и Nova (и между другими сервисами OpenStack и Nova) основано на взаимодействии через публичное API. Оно хорошо документировано, то есть на его основе можно разработать прокси-сервер со специальной обработкой некоторых запросов (у нас для вычисления эталона). Настроив конфигурации остальных сервисов OpenStack-based ВИ, возможно внедрить такой сервер в структуру OpenStack. Одной из проблем будет различение легальных пользователей и нарушителей, поскольку необходимо обрабатывать запросы в соответствии с правами пользователей. Для этого необходимо отдельно настроить взаимодействие прокси-сервера с сервисом OpenStack Keystone (в случае возникновения проблем с настройкой можно заменить OpenStack Keystone собственным сервисом аутентификации и авторизации, однако целесообразность разработки такого решения вызывает вопросы, так как сервис необходимо будет адаптировать к взаимодействию со всеми сервисами OpenStack). Еще одной проблемой может стать относительно большая задержка между проверкой КЦ конфигурации образа и запуском ВМ, поскольку после проверки КЦ запрос будет отправляться в другой сервис. Предложенное решение (из-за своей архитектуры: отправки запроса в другой сервис) не позволит существенно снизить задержку. Необходимо осуществлять проверку КЦ непосредственно перед запуском ВМ.

Для определения момента запуска KVM-based ВМ можно использовать libvirt. Libvirt– это наиболее часто используемый драйвер виртуализации в OpenStack [21]. OpenStack Nova для работы с ВМ использует libvirt, при поддержке программы QEMU (для эмуляции аппаратного обеспечения различных платформ) и, если доступен, KVM. Libvirt является свободной реализацией API гипервизора KVM и содержит набор дополнительных возможностей [22]. Одной из них являются хуки (программы). Libvirt позволяет запускать пользовательские хуки на определенные события libvirt, например, на запуск ВМ (/etc/libvirt/hooks/qemu) [23]. При выполнении хука libvirt передает ему некоторые параметры через аргументы командной строки. В зависимости от них можно понять статус (например, запуск или остановка ВМ) и имя ВМ. То есть создав подобный хук, можно отслеживать запуск ВМ и инициировать проверку КЦ образа ВМ непосредственно перед запуском ВМ. Подобная идея успешно реализуется в специальном программном обеспечении (СПО) СЗИ от несанкционированного доступа (НСД) «Аккорд-KVM» компании «ОКБ САПР» [24]. В случае нарушения КЦ администратор будет получать оповещение. Таким образом, использование хуков libvirt для отслеживания запуска ВМ является наилучшим решением для отслеживания событий запуска ВМ и ее создания из образа среди встраивания во внутреннюю очередь сообщений OpenStack Nova и прокси-сервера обработки запросов к Nova.

Теперь, зная имя запускаемой ВМ, необходимо получить образ, для которого необходимо посчитать эталон. Поскольку информация о ВМ хранится в части Nova DB сервиса OpenStack Nova, то исследуем этот компонент с целью нахождения информации о взаимосвязи между полем id таблицы images БД glance (GUID) и названием запускаемой ВМ. Получаем, что в БД nova содержится таблица instances с интересуемой информацией. В ней хранятся метаданные созданных ВМ в OpenStack-based ВИ, такие как статус, количество выделенной памяти, имя хост-компьютера и другие. С помощью полей hostname (display_name) и image_ref устанавливается взаимосвязь между именем ВМ и используемым

образом ВМ. Используя эту таблицу, можно установить соответствие между именем запускаемой ВМ, которое передается хуку libvirt в качестве аргумента командной строки, и образом ВМ, для которого необходимо посчитать эталон.

Было установлено, как проверять соответствие образа ВМ хранимому эталону. Перейдем к тому, как и когда создавать исходный эталон. Необходимо создавать исходный эталон для каждого образа ВМ в момент его добавления в OpenStack-based ВИ. Поскольку OpenStack Glance управляет хранением образов ВМ, то рассмотрим его устройство подробнее. В отличие от OpenStack Nova он не содержит нескольких внутренних серверов. Glance написан на Python и является HTTP сервером, его структура (схема) реализована через набор файлов-компонентов, каждый из которых обрабатывает запрос и направляет следующему [25]. То есть Glance состоит из набора “слоев”, каждый из которых реализует определенные функции и отправляет запрос на следующий “слой”. Существуют несколько способов для определения момента добавления образа ВМ. Аналогично рассматриваемому решению для OpenStack Nova можно сделать прокси-сервер для обработки запросов к Glance. В момент получения ответа от Glance прокси-сервер будет создавать исходный эталон, но возникает проблема, связанная с относительно большой задержкой между фактическим созданием записей в Glance DB и вычислением эталона. Другой способ – создание дополнительного слоя для Glance, который будет создавать эталон непосредственно до создания записей в БД. Однако это требует внедрения во внутреннюю структуру Glance, что усложнит поддержку разрабатываемого программного модуля при появлении новых версий OpenStack. Еще одним способом определения момента добавления образа ВМ является создание прокси-сервера для обработки запросов к самой БД. Данный способ позволит создавать исходный эталон сразу после добавления записей в БД. Еще одним его преимуществом является удобство конфигурирования, поскольку при его внедрении необходимо будет только изменить настройки БД в Glance (без изменения других сервисов OpenStack).

Таким образом, установлены события (моменты времени), когда будет происходить взаимодействие разрабатываемого программного модуля с эталонами конфигурации образов ВМ. Разработаны возможные способы внедрения в OpenStack, описаны их преимущества и недостатки. Выбрано использовать хуки libvirt для определения момента запуска ВМ и прокси-сервер для БД glance для определения момента добавления образов ВМ в сервис OpenStack Glance.

5. Архитектура модуля КЦ конфигураций образов ВМ. Разрабатываемая система должна внедряться на хост-компьютер ВИ, иметь доступ к сервисам OpenStack и предоставлять удобный способ управления настройками КЦ конфигураций образов ВМ. При создании системы можно использовать клиент-серверную архитектуру. Сервер будет запускаться на хост-компьютере ВИ до старта ВИ и будет принимать HTTP-запросы (от хука libvirt), которые вызовут либо добавление эталона в память, либо проверку КЦ конфигурации образа ВМ. Клиентом может являться веб-приложение, которое по протоколу WebSocket будет получать сообщение и уведомлять администратора в случае нарушения КЦ. Сервер в таком случае должен запрещать запуск ВМ. Еще одной частью системы будет хук libvirt, который при вызове отправит соответствующий HTTP-запрос на сервер с целью его уведомления о необходимости проверки КЦ образа запускаемой ВМ. Получив запрос, сервер обратится в БД nova, определит идентификатор образа ВМ. Используя его, вычислит эталон от значений таблиц БД glance сравнит значение с хранимым в памяти. В случае несовпадения значений сервер отправит широковещательное сообщение по WebSocket о нарушении КЦ конфигурации образа ВМ (сообщение получит администратор ВИ с установленным соединением). Подробная схема взаимодействия представлена на рисунке 3.

Для создания исходных эталонов в памяти прокси-сервер БД glance будет обрабатывать запросы в БД glance. В случае запросов создания (изменения) образов ВМ будет вычисляться и сохраняться эталон.

Подробная схема создания эталонов конфигураций образов ВМ представлена на рисунке 4.

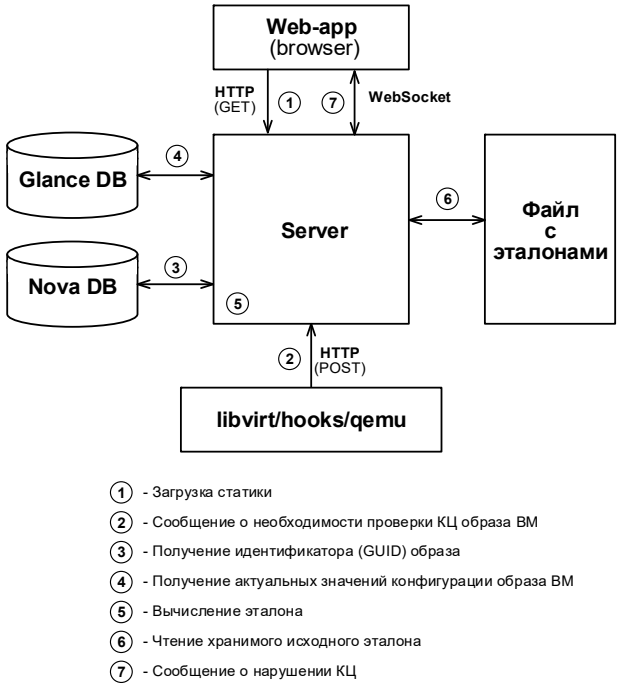


Рис. 3. Схема проверки КЦ конфигураций образов ВМ

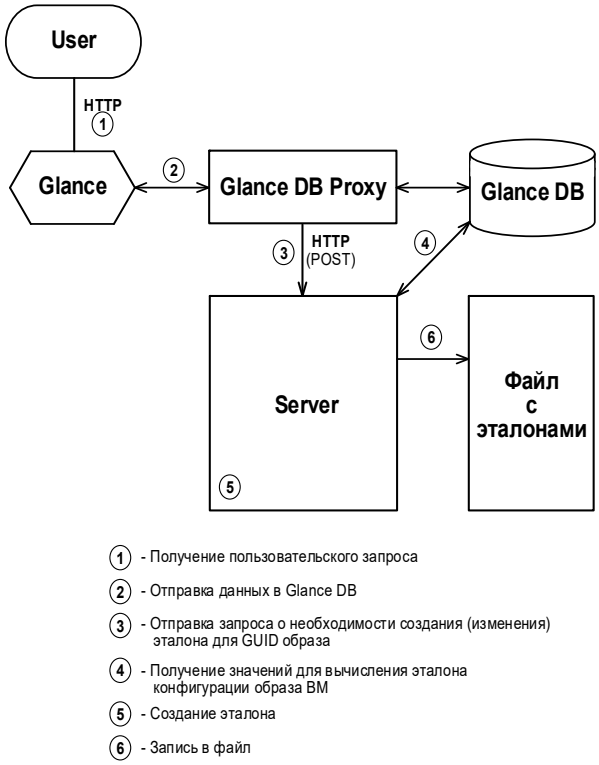


Рис. 4. Схема создания эталонов образов ВМ

Можно отметить, что особенностью разработанной архитектуры программного модуля для КЦ конфигураций образов ВМ является возможность внедрения КЦ содержимого файлов образов ВМ без необходимости внесения значительных изменений в архитектуру СЗИ.

Заключение. Получено решение одной из частей задачи КЦ ВМ в OpenStack – КЦ конфигураций образов ВМ. Описанная архитектура программного модуля реализует проверку конфигураций образов ВМ, хранимых в базе данных Glance DB платформы OpenStack, на соответствие с эталоном.

При развитии модуля для обеспечения КЦ конфигураций ВМ, хранимых в Nova DB, использования контрольных сумм в качестве эталона может оказаться недостаточным (поскольку в отличии от образов для одной ВМ значительно чаще может быть несколько разрешенных состояний), поэтому необходимо использовать атрибутные модели контроля доступа к КЦ конфигураций ВМ [19].

Список литературы

1. Защита виртуальной инфраструктуры // Официальный сайт компании Код Безопасности [Электронный ресурс]. – Режим доступа : https://www.securitycode.ru/upload/iblock/d0d/Virtualization_2018.pdf. – Дата доступа : 02.12.2020.

2. Image Signing and Verification Support: Blueprints: Glance [Электронный ресурс]. – Режим доступа : https://blueprints.launchpad.net/glance/+spec/image-signing-and-verification-support. – Дата обращения: 02.12.2020.

3. OpenStack Docs: Glance Image Signing and Verification // Официальный сайт спецификации OpenStack [Электронный ресурс]. – Режим доступа : https://specs.openstack.org/openstack/glance-specs/specs/mitaka/implemented/image-signing-and-verification-support.html. – Дата обращения: 02.12.2020.

4. Glance Image creation checksum logic – Ask OpenStack: Q&A Site for OpenStack Users and Developers [Электронный ресурс]. – Режим доступа : https://ask.openstack.org/en/question/90047/glance-image-creation-checksum-logic/. – Дата обращения: 02.12.2020.

5. Bugs: Glance [Электронный ресурс]. – Режим доступа : https://bugs.launchpad.net/glance/+bugs?field.tag=security. – Дата обращения: 02.12.2020.

6. Мозолина, Н. В. Разработка средства контроля целостности виртуальной инфраструктуры и ее конфигурации / Н. В. Мозолина // Выпускная квалификационная работа. – 2017. – С. 19–36.

7. Мозолина, Н. В. Контроль целостности виртуальной инфраструктуры и ее конфигурации / Н. В. Мозолина // Вопросы защиты информации. – 2016. – Вып. 3. – С. 31–33.

8. What is OpenStack? [Электронный ресурс] // Официальный сайт проекта OpenStack. – Режим доступа : https://openstack.org/software. – Дата обращения: 02.12.2020.

9. Журов, П. М. Разработка и исследование модели доступа к объектам облачных инфраструктур / П. М. Журов // Выпускная квалификационная работа. – 2019. – С. 18–22, 77–81.

10. OpenStack Docs: Swift Architectural Overview [Электронный ресурс] // Официальный сайт документации OpenStack. – Режим доступа : https://docs.openstack.org/swift/latest/overview_architecture.html. – Дата обращения: 02.12.2020.

11. OpenStack Docs: OpenStack Block Storage (Cinder) documentation // Официальный сайт документации OpenStack [Электронный ресурс]. URL: https://docs.openstack.org/cinder/latest/. – Дата обращения: 02.12.2020.

12. OpenStack Docs: Welcome to Glance's documentation! // Официальный сайт документации OpenStack [Электронный ресурс]. URL: https://docs.openstack.org/glance/latest/. – Дата обращения: 02.12.2020.

13. OpenStack Docs: Glance database architecture // Официальный сайт документации OpenStack [Электронный ресурс] URL: https://docs.openstack.org/glance/pike/contributor/database_architecture.html. – Дата обращения: 02.12.2020.

14. OpenStack Docs: Basic architecture // Официальный сайт документации OpenStack [Электронный ресурс] URL: https://docs.openstack.org/glance/pike/contributor/architecture.html. – Дата обращения: 02.12.2020.

15. OpenStack Docs: Image service overview // Официальный сайт документации OpenStack [Электронный ресурс] URL: https://docs.openstack.org/glance/latest/install/get-started.html. – Дата обращения: 02.12.2020.

16. OpenStack Docs: Tasks // Официальный сайт документации OpenStack [Электронный ресурс]. URL: https://docs.openstack.org/glance/pike/admin/tasks.html. – Дата обращения: 02.12.2020.

17. OpenStack Docs: Using Glance's Metadata Definitions Catalog Public APIs // Официальный сайт документации OpenStack [Электронный ресурс]. URL: https://docs.openstack.org/glance/pike/user/ glancemetadefcatalogapi.html. – Дата обращения: 02.12.2020.

18. Мозолина, Н. В. Задание эталона при контроле целостности конфигурации виртуальной инфраструктуры / Н. В. Мозолина // Новые информационные технологии и системы : сб. науч. ст. XII Междунар. науч.-техн. конф., Пенза. 23-25 ноября 2016. – С. 219–225.

19. Ерин, Ф. М. Построение шаблонов для решения задачи контроля целостности конфигурации на основе атрибутной модели контроля доступа / Ф. М. Ерин // Вопросы защиты информации. – 2018. – Вып. 3. – С. 3–6.

20. Миеттинен, М. Способ обеспечения целостности набора записей данных. Российский патент 2009 года RU 2351978 C2. Изобретение по МКП G06F11/08 [Электронный ресурс] / М. Миеттинен, К. Хятенен. – Режим доступа : https://patenton.ru/patent/RU2351978C2. – Дата обращения : 02.12.2020.

21. OpenStack Docs: Libvirt – Nova Virtualisation Driver // Официальный сайт документации OpenStack [Электронный ресурс]. – Режим доступа : https://docs.openstack.org/kolla-ansible/latest/reference/compute/libvirt-guide.html. – Дата обращения : 02.12.2020.

22. libvirt: Domain XML format // Официальный сайт проекта libvirt [Электронный ресурс]. – Режим доступа : https://libvirt.org/formatdomain.html. – Дата обращения : 02.12.2020.

23. libvirt: Hooks for specific system management // Официальный сайт проекта libvirt [Электронный ресурс]. – Режим доступа : https://libvirt.org/hooks.html. – Дата обращения : 02.12.2020.

24. Специальное программное обеспечение средств защиты информации от несанкционированного доступа «Аккорд-KVM». Руководство администратора безопасности информации // Официальный сайт компании ОКБ САПР [Электронный ресурс]. – Режим доступа : https://www.okbsapr.ru/upload/iblock/786/786f40d485a08e160fca07f38 fbd78e6.pdf. – Дата обращения : 02.12.2020.

25. OpenStack Docs: Glance domain model implementation // Официальный сайт документации OpenStack [Электронный ресурс]. – Режим доступа : https://docs.openstack.org/glance/latest/contributor/domain_implementation.html. – Дата обращения : 02.12.2020.

УДК 004.056.55

ПРАКТИЧЕСКИЕ ВОПРОСЫ ОРГАНИЗАЦИИ ДИСКОВОГО ШИФРОВАНИЯ

М.В. ЕГОРОВА
Белорусский государственный университет, г. Минск, Республика Беларусь

Введение. В настоящее время вопрос безопасности и защиты персональных и корпоративных данных стоит как никогда остро. Одним из вариантов обеспечения конфиденциальности данных, хранящихся на различных носителях информации, является дисковое шифрование. Дисковое шифрование – это технология защиты данных, основанная на применении методов симметричной криптографии, после использования которых хранящаяся на диске информация становится неотличимой от случайной последовательности. Без знания ключа шифрования защищенные данные являются недоступными для всех пользователей (как регулярных, так и злоумышленников). Дисковое шифрование производится при помощи программных и аппаратных средств, шифрующих каждый байт хранилища. Однако на рынке не представлены средства, использующих криптографические алгоритмы, спецификации которых приняты в качестве ТНПА Республики Беларусь. В данном тексте рассматриваются вопросы практической организации дискового шифрования, соответствующего национальным криптографическим стандартам [2–5], защиты контейнера от атаки путем перебора пароля пользователя, эффективной блокировки контейнера и контроля целостности.

1. VeraCrypt. Проектирование таких комплексных и масштабных проектов – трудоемкая задача, требующая большого количества ресурсов, а также знания особенностей дисковой архитектуры различных ОС. Поэтому оптимальным является решение усовершенствовать готовую реализацию с открытым исходным кодом и свободной лицензией – выбор пал на программное обеспечение VeraCrypt [1]. Это решение обеспечивает простоту встраивания необходимых криптографических алгоритмов, кроссплатформенность, а также определенные гарантии безопасности в силу проведения независимого аудита исходного кода. VeraCrypt позволяет создавать защищенные контейнеры, в том числе скрытые, и работать с ними с использованием шифрования «на лету». Это означает, что данные автоматически зашифровываются прямо перед сохранением и расшифровываются сразу после загрузки без вмешательства пользователя. Схема работы VeraCrypt представлена на рисунке 1. Первые 512 байт соответствуют заголовку базового контейнера, а байты с 65536 по 66047 – заголовку скрытого контейнера.

Рис. 1. Схема монтирования VeraCrypt

2. Стандарты. Стандарт 34.101.31-2020 [2] определяет семейство криптографических алгоритмов шифрования и контроля целостности, которые используются для защиты информации при ее хранении, передаче и обработке. Для соответствия разрабатываемого ПО данному стандарту планируется добавить в исходный код программной реализации следующие алгоритмы: belt-block (пункт 6.1), belt-hash (пункт 7.8), belt-bde и belt-sde (пункт 7.9).

В данных режимах, как и в распространенном режиме XTS синхропосылка вырабатывается детерминировано, исходя из смещения сектора и ключа, а ее модификация выполняется с помощью умножения в кольце многочленов. В качестве функции хэширования предлагается использовать bash из СТБ 34.101.77-2020 [4] с уровнем стойкости $l = 128$. Это решение обусловлено результатами исследования, в ходе которого было определено, что функция хэширования bash256 в 3-4 быстрее функции хэширования belt-hash.

3. Разделение секрета. Одной из основных проблем, стоящих перед дисковым шифрованием, является управление паролями. Ключ шифрования диска защищен паролем пользователя, который часто имеет низкую энтропию. Таким образом, сложность раскрытия защищенной информации не превышает сложности раскрытия пароля пользователя путем перебора. Для усиления безопасности предлагается добавить возможность защиты пароля путем разделения секрета. Задача разделения секрета подразумевает под собой разделение секретной информации (общего секрета) на несколько частичных секретов таким образом, что только имея заранее заданное число частичных секретов участники могут ее восстановить, следовательно, вероятность компрометации информации снижается. Таким образом, предлагается вместо пароля пользователя сгенерировать высокоэнтропийный ключ P длины 256 бит и применить $(k, n)-$ пороговую схему разделения секрета в соответствии с СТБ 34.101.60-2014 [3], то есть разделить ключ P на n, $(n \le k)$ частей и обеспечить их хранение на различных носителях, где k, $(k \ge 2)$ – необходимое для восстановления секрета количество долей. В соответствии со стандартом с СТБ 34.101.78-2019 [5] (раздел 11), частичные секреты могут сохраняться во вспомогательных контейнерах, защищенных на паролях. Пароли защиты различных контейнеров могут совпадать. В любой комбинации порогового числа частичных секретов хотя бы один из них должен быть защищен на пароле.

4. Пароль уничтожения. Еще одной предлагаемой модификацией VeraCrypt является добавление пароля уничтожения, который может быть опционально задан пользователем при создании контейнера. В экстренной ситуации и в случае необходимости быстрой и безопасной перманентной блокировки контейнера пользователь вводит вместо обычного пароля пароль уничтожения, в результате чего 512 байт соответствующего заголовка контейнера принудительно заполняются последовательностью байт вида 0x00, что приводит к невозможности восстановления информации любыми способами кроме полного перебора множества ключей мощностью 2^{256}. Технически это выглядит следующим образом: при создании контейнера у пользователя запрашивается 2 пароля, один из которых используется в качестве обычного, а второй для уничтожения данных. После инициализации контейнера заголовок расшифровывается на пароле уничтожения и первые 32 байта, называемые в дальнейшем R, добавляются перед началом заголовка. При попытке осуществления штатного монтирования первые 32 байта расшифрованного заголовка будут сравниваться с хранящимся перед заголовком R и при полном совпадении контейнер приводится в негодность описанным выше способом. В противном случае монтирование продолжается как обычно. Для скрытого тома осуществляются аналогичная последовательность действий.

5. Механизмы контроля целостности. Иногда при использовании дискового шифрования возникает необходимость не только сохранять конфиденциальность данных, но и контролировать их целостность. Однако популярное ПО, применяемое для дискового шифрования, никак не контролирует целостность зашифрованных данных.

Как правило, при разработке хэш-функций используются итерационные методы. В качестве примера можно привести конструкцию Меркла-Дамгарда, используемую при разработке таких известных хэш-функций, как MD5, SHA-1 и SHA-2. Тем не менее такие схемы имеют существенный недостаток – линейный характер вычислений: даже если в файл, целостность которого мы контролируем, были внесены лишь минимальные изменения (например, изменился последний байт), хэш-значение будет пересчитываться для всего файла целиком. Такой подход не подходит для контроля целостности контейнеров VeraCrypt, поэтому предлагается использовать один из следующих вариантов: древовидное хэширование или инкрементальное хэширование.

5.1. Древовидное хэширование. Рассмотрим древовидное хэширование [7]. Алгоритм древовидного хэширования действует следующим образом: на вход подаются данные,

разбиваемые на блоки одинаковой длины. Затем вычисляется хэш-значение каждого блока данных. После чего к хэш-значениям применяются односторонние функции свертки: два сконкатенированных хэш-значения подаются в хэш-функцию. Данный процесс можно описать в виде бинарного дерева. Таким образом, листьям такого дерева будут соответствовать хэш-значения блоков данных, а остальным узлам – промежуточные значения сверток. Вершина – итоговое хэш-значение. Данный подход легко обобщается на случай k-деревьев, где каждый неконечный узел имеет k исходящих ребер.

Такая структура обладает следующими свойствами: относительно небольшая высота дерева пропорциональна $\log_k n$, где n – количество блоков данных; независимость вычисления поддеревьев.

При условии, что на базе n блоков (листьев) получается полное k-дерево, число операций хэширования будет равно $N = \frac{k^{\log_k n+1} - 1}{k-1}$.

Еще одной особенностью представления алгоритмов хэширования в виде дерева является независимость итогового результата от порядка свертывания поддеревьев, что предоставляет возможность использования методов параллельных вычислений при первом вычислении узлов дерева. Которые, в свою очередь, значительно сокращают время получения результата.

Для выяснения особенностей контроля целостности с помощью метода древовидного хэширования было проведено исследование с использованием хэш-функции bash256, реализованной в соответствии с эталонным вариантом из библиотеки bee2. В ходе исследования были получены следующие результаты.

Так как в алгоритме хэш-функции bash256 отсутствуют операции, скорость выполнения которых может зависеть от входных данных, то скорость хэширования не зависит от содержания хэшируемых данных, при этом время хэширования прямо пропорционально объему хэшируемых данных.

Для выяснения оптимального размера буфера p были вычислены хэш-значения файла размером 1 ГБ с размером буфера от 32 Б до 16 МБ.

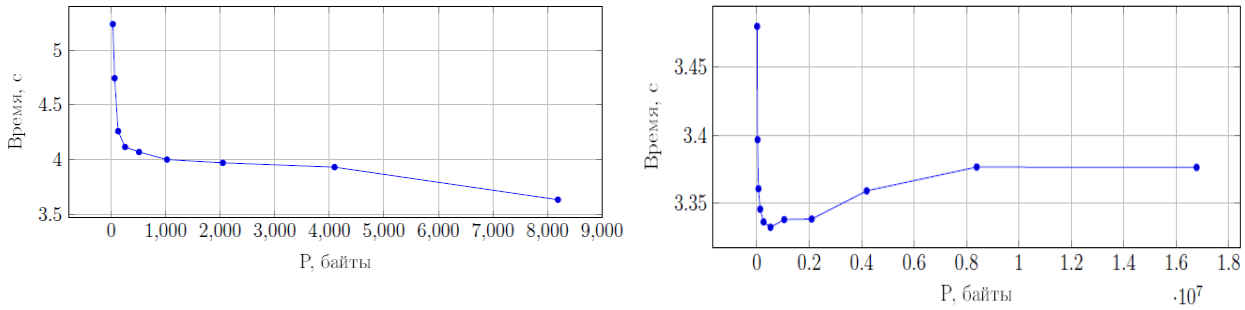


Рис. 2. Графики зависимости времени хэширования от размера буфера

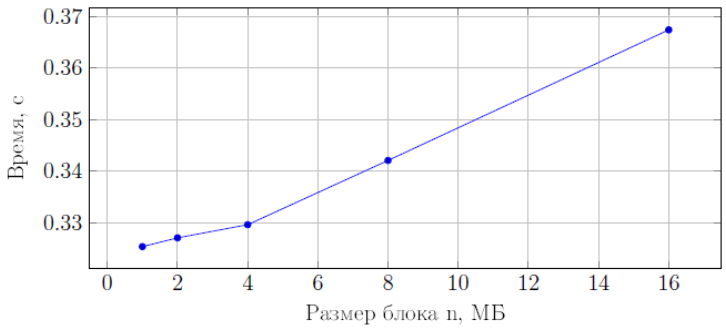


Рис. 3. График зависимости времени хэширования от размера разбиения

Для дальнейших экспериментов оптимальным принят размер буфера равный 1 МБ. Для выяснения оптимального размера разбиения n были вычислены хэш-значения файла размером 100 МБ с размером разбиения от 1 МБ до 16 МБ.

Оптимальным принят размер разбиения равный 1 МБ, так как разница между временем для n = 1, 2, 4 МБ составляет менее 5%.

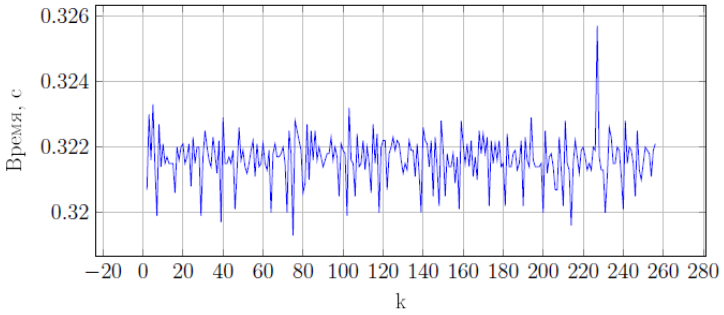


Рис. 4. График изменения времени хэширования при различных k

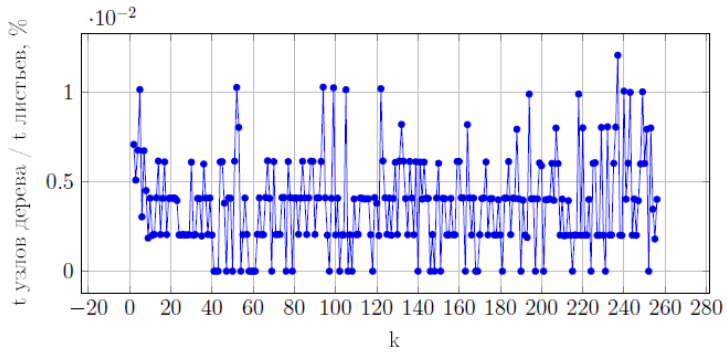


Рис. 5. График времени расчета узлов дерева / время хэширования листьев для различных k

Для выбранного оптимальными буфера и размера разбиения были построены k-деревья, где k изменялось от 2 до 256. Исходя из результатов, отображенных на рисунке 4, следует, что выбор k мало влияет на итоговое время работы (изменения колеблются в пределах 2%, что можно списать на погрешность вычислений).

Согласно результатам, представленным на рисунке 5, можно утверждать, что все процентные сополагать оптимальными.

Принято решение выбрать $k = 2$ в качестве оптимального, то есть использовать бинарное дерево.

В качестве демонстрации преимущества метода древовидного хэширования перед хэшированием всех данных целиком произведено хэширование файла размером 30 ГБ для оптимальных параметров (p = 1 МБ, размер разбиения равен 1 МБ, $k = 2$). В результате время расчета дерева на 1–2 % больше времени хэширования всего файла, а время пересчета итогового хэш-значения при изменении 1 блока данных при древовидном хэшировании составило 0.002–0.003 % от времени хэширования файла целиком.

С учетом того, что при пересчете итогового хэш-значения при изменении одного блока данных основное время тратится на вычисление хэш-значения самого блока, а время пересчета узлов дерева незначительно, то можно полагать, что время пересчета итогового хэш-значения при изменении одного блока данных с помощью древовидного хэширования в n раз быстрее, чем путем хэширования файла целиком. Так как с увеличением объема данных, соответственно, увеличивается и число блоков, то, очевидно, что при увеличении объема входного файла разница в скорости между вычисление хэш-значения всего файла и пересчетом хэш-значения файла с использованием предварительно вычисленного дерева возрастает.

Подводя итоги, в ходе исследования были найдены следующие оптимальные параметры для древовидного хэширования: p = 1 МБ, n = 1 МБ, $k = 2$.

5.2. Схема инкрементального хэширования. Схема инкрементального хэширования [8] работает по следующему алгоритму:

1. Для каждого блока данных одинаковой длины M_i, $i = 1, \ldots, n$, вычисляется дополненный блок $\overline{M_i} = M_i \,||\, ID_i$, $ID_i = <i>$.

2. Для каждого дополненного блока M_i вычисляется хэш-значение $y_i = h\left(\overline{M}_i\right), i = 1,\ldots,n$, где h – хэш-функция с выходом длины k. Длина выхода кратна 64 (для уровня стойкости 128 или 256 бит k должно быть больше 2000 бит, например, хэш-функции SHAKE128 и SHAKE256).

3. Итоговое хэш-значение получается путем сложения промежуточных хэш-значений.

При изменении части исходных данных нет необходимости пересчитывать хэш-значения для каждого блока. Требуется лишь подсчитать $y'_i = h\left(\overline{M'_i}\right)$ и $y_i = h\left(\overline{M_i}\right)$, где $\overline{M'_i}$ – измененный дополненный блок, $\overline{M_i}$ – исходный дополненный блок. А затем вычислить $y' = y - y_i + y'_i$, где «-» и «+» 64-битные операции сложения и вычитания.

Так как в РБ не стандартизированы хэш-функции с выходом длины больше 2000 бит, то остановимся на варианте древовидного хэширования.

Заключение. Подводя итоги, написание программного обеспечения с добавлением вышеперечисленных модификаций позволяет создать конкурентоспособное приложение, соответствующее белорусским стандартам и имеющее усиленные по сравнению с оригиналом гарантии безопасности.

1. Для усиления безопасности предлагается добавить возможность защиты пароля путем разделения секрета.

2. В качестве механизма контроля целостности рекомендуется использовать схему древовидного хэширования.

3. Предложен механизм экстренной блокировки контейнера.

Список литературы

1. Официальная документация программы VeraCryp, Ноябрь 2020 [Электронный ресурс]. – Режим доступа : https://www.veracrypt.fr/en/Documentation.html. – Дата доступа : 07.12.2020.

2. СТБ 34.101.31-2020. Информационные технологии и безопасность. Криптографические алгоритмы шифрования и контроля целостности – Минск : БелГИСС, 2020.

3. СТБ 34.101.60-2014. Информационные технологии и безопасность. Алгоритмы разделения секрета – Введ. 2014 – Минск : БелГИСС, 2014.

4. СТБ 34.101.77-2020. Информационные технологии и безопасность. Алгоритмы хэширования – Введ. 2014 – Минск : БелГИСС, 2020.

5. СТБ 34.101.78-2019. Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей – Введ. 2019 – Минск : БелГИСС, 2019.

6. Recommendation for Block Cipher Modes of Operation: The XTS-AES. Mode for Confidentiality on Storage Devices, NIST Special Publication 800-3E, [Electronic resource] / Morris Dworkin, January 2010. – Режим доступа : http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf. – Дата доступа : 20.03.2021.

7. Гапанович, Д. А. Современные информационные технологии и ИТ-образование. Хэш-алгоритмы с управляющей древовидной структурой и метод его реализации на параллельных архитектурах / Д. А. Гапанович, В. Н. Чубариков. – М. : МГУ, 2017.

8. Mihajloska, H. Reviving the idea of incremental cryptography for the zettabyte era use case: Incremental hash functions based on SHA-3, [Electronic resource] / H. Mihajloska, D. Gligoroski, S. Samardjiska. – Режим доступа : http://eprint.iacr.org/2015/1028. – Дата доступа : 02.04.2021.

УДК 537.531:621.039.537-037.87

МЕТОДИКА ИЗГОТОВЛЕНИЯ ГИБКИХ ЭКРАНОВ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ НА ОСНОВЕ СЕТЧАТЫХ СТРУКТУР

Б.И. ДУМЧЕВ, Е.С. БЕЛОУСОВА, С.Э. САВАНОВИЧ
Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Беларусь

Введение. Бурное развитие приборостроения, появление новых технологий беспроводной передачи данных привело к острой необходимости использования экранирующих материалов, которые защищают не только аппаратуру, но и персонал от электромагнитного излучения и различного рода электромагнитных помех. При этом выбор материала зависит от способа его применения, так, например, при строительстве или модернизации помещений используют различные пластины и сетки, фольгированные материалы и облицовочные панели, которые размещают в стенах под облицовочным слоем. При выборе материала для экранирования электромагнитного излучения определяют, насколько он соответствует требуемой эффективности экранирования в определенном диапазоне частот. Необходимо отметить, что такие материалы обладают отражающими и/или поглощающими свойствами. Так, например, пластины и сетки изготавливают из материала с низким электросопротивлением. Более эффективными являются экраны электромагнитного излучения (ЭМИ), изготовленные из проволочной сетки или из тонкой (толщиной 0,01-0,05 мм) алюминиевой, латунной или цинковой фольги.

На сегодняшний день на мировом рынке существует огромное разнообразие экранирующих электромагнитное излучение сетчатых материалов на основе стали [1–3], меди [4], латуни и бронзы [5], никеля [6] а также полиэстерных нитей с добавлением меди [7]. Большинство производителей таких материалов гарантируют ослабление порядка 40 дБ и эффективность экранирования около 90 %, долговечность и устойчивость к разных погодным условиям. При этом не все производители отмечают, что при использовании таких материалов требуется дополнительное заземление. Кроме того, экранирование низкочастотных электромагнитных полей практически не обеспечивается сетчатыми материалами. Также необходимо отметить такие недостатки как большая масса и невозможность придания любой заданной формы, трудоемкость изготовления.

В источнике [8, с.83] доказано, что отражающее действие всех видов сеток при прочих равных условиях тем лучше, тем меньше величина χ, определяемая по следующей формуле:

$$\chi = 2b \cdot \lambda^{-1} \cdot \ln(b \cdot \pi \cdot r_0/2), \quad (1)$$

где b – размер стороны квадратной ячейки; r_0 – радиус проводника; λ – длина волны падающего излучения.

Таким образом, можно сделать вывод, что коэффициент отражения сетчатого экрана электромагнитного излучения тем больше, чем меньше размеры его ячеек.

Целью данной работы была разработка экрана электромагнитного излучения на основе сетчатой структуры из углеродного порошка для армирования стен помещений с целью ослабления внешнего электромагнитного излучения.

В качестве основного материала для экрана электромагнитного излучения был выбран стеклотканевый холст, который представляет собой полотно, сплетенное из стеклянных нитей, полученных при температуре 1200 ºС и обработанных специальным растворами для обеспечения прочности. Такой материал обладает следующими свойствами: гибкость, прочность, долговечность, экологически чистый, не накапливает статического электричества, устойчив к открытому пламени, перепадам температур, высокой влажности и различным химическим веществам. Обычно стеклотканевый холст используется для качественной и прочной отделки внутренних поверхностей помещений для предотвращения появления трещин. Таким образом данным материал подходит для поставленной цели и является хорошей основой для создания экрана электромагнитного излучения.

Сетчатая структура формировалась путем нанесения на стеклотканевый холст порошка углерода горизонтальными и вертикальными линиями в двух взаимноперпендикулярных направлениях. По представленной формуле (1) было определено, как изменяется значение χ при разных значения частоты в диапазоне 2–17 ГГц и разных размерах ячеек (от 1 до 5 см), при толщине линии не более 5 мм. Как видно из рисунка 1, значение χ действительно уменьшается при увеличении частоты и увеличение размера ячейки. При это необходимо помнить, что чем больше размер ячейки, тем меньше коэффициент предачи. Для исследования закономерности изменения размера стороны квадратной ячейки на частотные характеристики коэффициентов отражения и передачи были изготовлены экраны электромагнитного излучения на основе сетчатой структуры с размерами ячейки 1 и 2 см.

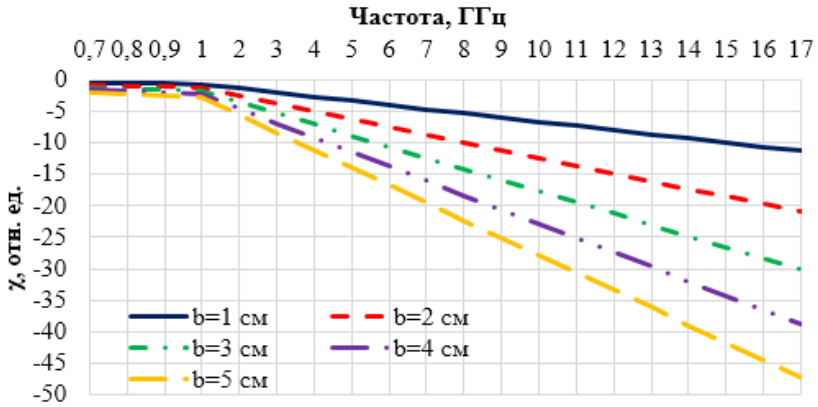


Рис. 1. Зависимость величины χ от размера стороны квадратной ячейки (*b*) и частоты

Методика изготовления экрана электромагнитного излучения на основе сетчатой структуры из углеродного порошка включает следующие этапы:

− определение требуемых размеров экрана ЭМИ;

− раскрой стеклотканевого полотна и его подготовка к нанесению клея, предварительно разделив полотно на две равные части;

− нанесение клея на стеклотканевый холст слоем толщиной 0,5 мм;

− подготовка порошка технического углерода и наполнение рукава для фугования;

− нанесение технического углерода на половину стеклотканевого холста вертикальными и горизонтальными взаимоперпендикулярными линиями до получения углеродной сетки с помощью рукава для фугования;

− склеивание двух частей холста по предварительной разметке (рис. 2);

− удаление излишков клея, образовавшихся после склеивания двух частей холста;

− проверка качества полученного экрана ЭМИ, качества адгезии порошкообразного материала со связующим веществом и полотном, соответствия сформированного изделия необходимым экранирующим характеристикам.

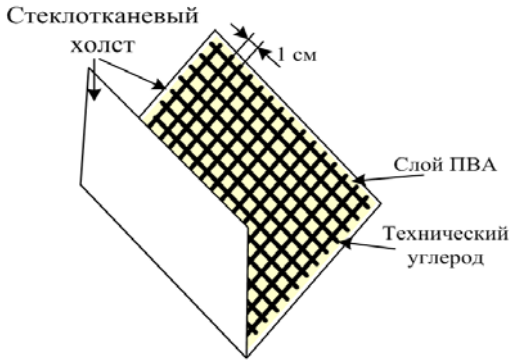


Рис. 2. Экран электромагнитного излучения на основе сетчатой структуры из углеродного порошка

Для измерения коэффициентов передачи и отражения конструкций экранов ЭМИ использовался панорамный измеритель коэффициентов передачи и отражения SNA 0,01–18, работающий по принципу раздельного выделения и непосредственного детектирования уровней падающей и отраженной волн. В состав панорамного измерителя входят:

– генератор качающейся частоты;

– блок обработки измерительных сигналов;

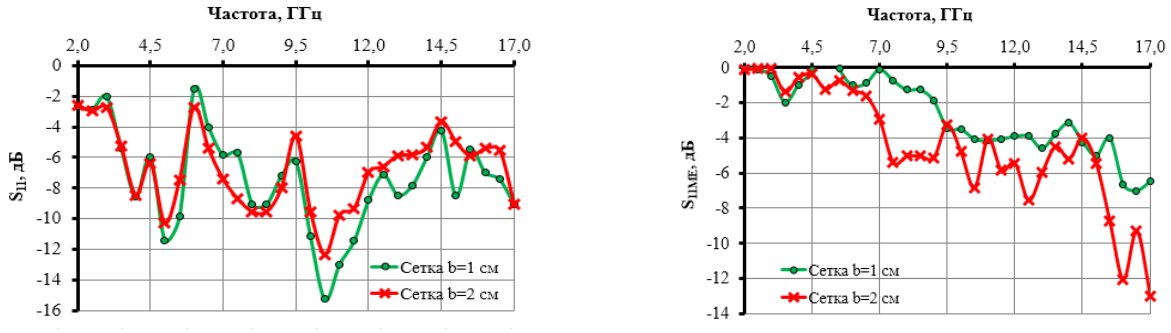
– передающая и приемная антенны;

– блоки направленных ответвителей (блоки в и A/R), предназначенные для выделения и детектирования падающей, отраженной и прошедшей электро-

магнитных волн и соединяющиеся с каналами блока обработки измерительных сигналов и антеннами.

Рабочий диапазон частот панорамного измерителя – 0,01–18 ГГц. Измерения выполнялись в автоматическом режиме на частотах диапазона 2–17 ГГц с шагом 0,063 ГГц. Для задания начальных параметров измерений (диапазона частот, вида измеряемого параметра) и систематизации его результатов использовалось специальное программное обеспечение.

На основе представленной выше методики было изготовлено 2 образца экрана электромагнитного излучения на основе сетчатой структуры из углеродного порошка с разными размерами стороны квадратной ячейки (1 и 2 см). Результаты измерения коэффициента отражения в режиме короткого замыкания показали, что у образца экрана электромагнитного излучения с размером ячейки $b = 2$ см коэффициент отражения составляет –5,4 … –13 дБ в диапазоне частот 7–17 ГГц. У образца экрана электромагнитного излучения с размером ячейки $b = 1$ см значения коэффициента отражения больше на 5–6 дБ в диапазоне частот 7–17 ГГц. При этом коэффициент передачи и коэффициент отражения, измеренный в режиме согласованной нагрузки, у образцов экрана электромагнитного излучения на основе сетчатой структуры практический одинаковый (рис. 2, 3). Таким образом, можно сделать вывод, что размер ячейки действительно влияет на величину коэффициента отражения, измеренного в режиме короткого замыкания, увеличение размера ячейки на 1 см способствует уменьшению коэффициента отражения больше на 5–6 дБ в диапазоне частот 7–17 ГГц.



а *б*

Рис. 3. Частотные зависимости коэффициентов отражения, измеренные в режиме согласованной нагрузки (*а*) и короткого замыкания (*б*), для образцов экрана ЭМИ на основе сетчатой структуры из углеродного порошка с разными размерами стороны квадратной ячейки

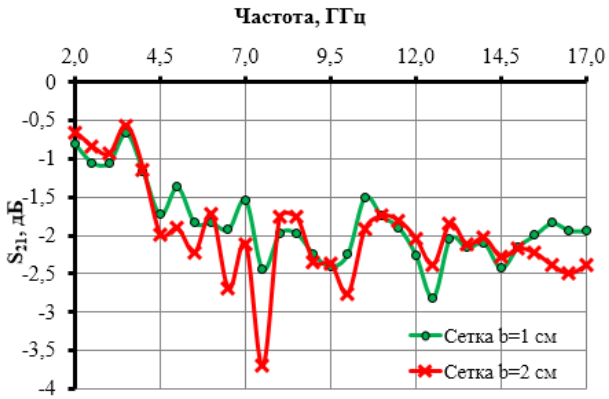


Рис. 4. Частотные зависимости коэффициентов передачи для образцов экрана ЭМИ на основе сетчатой структуры из углеродного порошка с разными размерами стороны квадратной ячейки

Заключение. Таким образом, можно утверждать, что изготовленный по предложенной методике экран ЭМИ на основе сетчатой структуры из углеродного порошка, нанесенного на стеклотканевый холст вертикальными и горизонтальными взаимоперпендикулярными линиями, может быть использован при строительстве, модернизации помещений, как основа для армирования стен, а также для ослабления внешних электромагнитных полей на 3 дБ в диапазоне частот 2–17 ГГц. Кроме того, данный экран электромагнитного излучения может быть использован для облицовочных панелей в сочетании с другими поглощающими ЭМИ материалами, что планируется исследовать авторами в продолжении данного исследования.

Список литературы

1. Экранирующая решетка V4A3 / NanoMarket [Электронный ресурс] – Режим доступа : https://nanomarket.ua/ru/ekranuucha-rishitka-v4a3-vchnch-55-db-rozmiri-0.9kh1-m/.

2. Экранирующая решетка V4A10 / NanoMarket [Электронный ресурс] – Режим доступа : https://nanomarket.ua/ru/ekranuucha-rishitka-v4a10-vchnch-40-db-rozmiri-1kh1-m/.

3. Экранирующая защитная сетка Aaronia A2000+ / ООО «Альт» [Электронный ресурс] – Режим доступа : http://www.alt-1c.ru/pages.html?id=5&cat=290&item=817.

4. Экранирующая сетка медная / ООО «Измерительные Системы и Технологии» [Электронный ресурс]. – Режим доступа : http://izlucheniya.ru/shop/ekraniruyushhaya-setka-mednaya-tkanaya-yachejka-0-56-mm/.

5. Сетки медные для экранирования помещений [Электронный ресурс] / ООО «Компания ИТЭРА». – Режим доступа : https://www.itera-setka.com.ua/сетка-каталог-сетки-медные-для-экранирования-помещений-тканые.

6. Орешко, С. М. Слоистый поглотитель электромагнитных волн и способ его изготовления / С. М. Орешко [и др.]. – Пат. РФ 2580408.

7. Swiss Shield New Daylite EMF Shielding Fabric / EMF Clothing Ltd [Электронный ресурс] – Режим доступа : https://emfclothing.com/en/emf-shielding/28-swiss-shield-new-daylite-emf-shielding-fabric.html.

8. Конторович, М. И. Электродинамика сетчатых структур / М. И. Конторович [и др.]. – М. : Радио и связь, 1987.

УДК 003.26+004.032.26

ПРИМЕНЕНИЕ ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫХ НЕЙРОННЫХ СЕТЕЙ В ЗАДАЧАХ СТЕГАНОГРАФИИ

О.Д. ЮШКЕВИЧ, М.В. МАЛЬЦЕВ
Белорусский государственный университет, г. Минск, Республика Беларусь

Введение. Стеганография – направление криптологии (в широком смысле), цель которого – разработка средств передачи и хранения информации, скрывающих сам факт ее передачи или хранения [1]. Для достижения этой цели секретное сообщение встраивается в контейнер – данные, которые передаются или хранятся в открытом виде. В качестве контейнера как правило используются изображения, аудио и видео файлы, при этом встроенное секретное сообщение не обнаруживается человеческими органами чувств. Таким образом, секретные данные скрываются от пассивного наблюдателя и для их извлечения требуются специальные методы. Существуют различные подходы к построению таких методов: так называемый «слепой» стегоанализ используется, если математическая модель данных неизвестна [2], значимые для теории и практики результаты получены с помощью вероятностно-статистического моделирования [3, 4]. В настоящей работе для решения задач стеганографии применяются математические модели, доказавшие свою эффективность для решения многих практических задач, – нейронные сети.

1. Постановка задачи. Путь имеется контейнер C, представляющий собой изображение в формате RGB с разрешением $W \times H$ пикселей, состоящее из трех цветовых 8-битных каналов. Рассматривается задача встраивания в контейнер C секретного сообщения $M \in \{0,1\}^{d \cdot W \cdot H}$ длиной $d \cdot W \cdot H$ бит (короткие сообщения дополняются незначащими нулевыми битами), где $d \in \{1, 2, ..., 24\}$ – параметр, характеризующий число бит, встроенных в один пиксель контейнера C, который будем называть глубиной кодирования (максимальное значение $d = 24$ означает, что исходное изображение C полностью заменяется другим изображением, которое соответствует секретному сообщению M). Имеются два алгоритма: кодировщик E и декодировщик D. Кодировщик получает на вход контейнер C и сообщение M и выдает на выходе контейнер C' со встроенным в него сообщением M: $E(C, M) = C'$. Декодировщик получает на вход C' и выдает на выходе сообщение M: $D(C') = M$. Рассматриваемая в настоящей статье задача стеганографии состоит в разработке использующего нейронные сети алгоритма встраивания секретного сообщения M в контейнер C.

2. Архитектура генеративно-состязательной нейронной стеганографической сети. Для решения задачи стеганографии в настоящей статье используются генеративно-состязательные нейронные сети (generative adversarial network, GAN), предложенные сотрудником компании Google Яном Гудфеллоу (Ian Goodfellow) [5]. В базовом варианте данной модели имеются две нейронные сети: генератор и дискриминатор. Генератор порождает объекты, принадлежащие различным классам, а дискриминатор пытается отличать объекты из разных классов. В настоящей статье рассматривается более сложная модель, состоящая из трех нейронных сетей: Кодировщика, Декодировщика и Критика, структура которых приведена далее.

Основными строительными блоками используемых нейронных сетей являются сверточные слои. Свертка изображения $I = (I_{ij})$ (матрица размерности $W \times H$) по ядру $K = (K_{ij})$ (матрица размерности $w \times h$, $w \le W, h \le H$) представляет собой линейный фильтр, который проходит по изображению и ставит в соответствие ($w \times h$)-матрице пикселей число по следующему правилу:

$$(I * K)_{xy} = \sum_{i=1}^{w} \sum_{j=1}^{h} K_{ij} \cdot I_{x+i-1, y+j-1}, \; 1 \le x \le W - w + 1, \; 1 \le y \le H - h + 1. \qquad (1)$$

В процессе обучения нейросеть определяет оптимальное значение *K*, минимизируя заданную функцию потерь. На практике это приводит к тому, что сверточный слой учится выделять определенные признаки, и чем глубже находится слой, тем более абстрактные признаки он выделяет. Первые слои как правило выделяют общие признаки, такие как изменения контраста, формы, резкость изображения, границы изображения. Комбинируя эти слои, становиться возможным понижать размерность изображения и извлекать из него полезные признаки.

Архитектура Кодировщика. Кодировщик *E* получает на вход исходное изображение с и сообщение $M \in \{0,1\}^{d \cdot W \cdot H}$. Задача Кодировщика – встроить *M* в *C* таким образом, чтобы Критик не обнаружил факта встраивания. Важно отметить, что значение параметра *d* может регулироваться на этапе инициализации сети. Рассмотрим три варианта архитектуры Кодировщика. Обозначим: $Conv_{i \to j}(\mathrm{X})$ – операция применения к изображению *X*, состоящему из *i* каналов, *j* операций свертки (1), в результате чего формируется *j*-канальное изображение. Параметры ядер свертки вычисляются в ходе обучения нейронной сети, о котором сказано далее (начальные значения ядер генерируются случайным образом).

Для всех вариантов архитектуры Кодировщика общими являются следующие начальные операции:

1. Обработка изображения с сверточным блоком:

$$\alpha = Conv_{3 \to 32}(C).$$

2. Конкатенация секретного сообщения *M* и полученной свертки (операция конкатенации обозначена ||), обработка полученного тензора сверточным блоком:

$$\beta = Conv_{32 \to 32}(\alpha \,||\, \mathrm{M}).$$

3. Последовательное применение сверточных блоков к тензору β:

$$C' = E(C, M) = Conv_{32 \to 3}(Conv_{32 \to 32}(\beta)).$$

На последнем (третьем) шаге формируется изображение C' со встроенным секретным сообщением *M*.

Второй вариант архитектуры кодировщика, которого обозначим E_r (от англ. residual – остаток) основан на работе [6], в которой показано, что остаточные связи как правило улучшают сходимость и устойчивость алгоритма, поэтому предполагается, что их использование улучшит качество изображения со встроенным секретным сообщением: C' формируется следующим образом (знак + здесь означает попиксельное сложение изображений):

$$E_r(C, M) = C + Conv_{32 \to 3}(Conv_{32 \to 32}(\beta)).$$

В третьем варианте архитектуры кодировщика, которого обозначим E_d (от англ. Dense – плотный), используются дополнительные связи между всеми слоями, что позволяет слоям на разных уровнях использовать признаки других уровней. Формально это записывается следующим образом:

$$\gamma = Conv_{64d \to 32}(\alpha \,||\, \beta \,||\, M),$$

$$\delta = Conv_{96d \to 3}(\alpha \,||\, \beta \,||\, \gamma \,||\, M),$$

$$E_d(C, M) = C + \delta.$$

Результатом каждого варианта является изображение C', содержащее секретное сообщение *M* и имеющее те же характеристики разрешения и глубины, что и исходное изображение (контейнер) *C*.

Архитектура Декодировщика. Декодировщик *D* получает на вход изображение C' и возвращает некоторое сообщение $\hat{M}$. Задача обучения нейронной сети состоит в том, чтобы добиться совпадения $\hat{M}$ и *M*, т. е. того, что Декодировщик верно восстанавливает секретное сообщение *M*. В ходе работы Декодировщика выполняются следующие операции:

$$\alpha = Conv_{3\to 32}(C'),$$

$$\beta = Conv_{32\to 32}(\alpha),$$

$$\gamma = Conv_{64\to 32}(\alpha \| \beta),$$

$$D(C') = Conv_{96\to dWH}(\alpha \| \beta \| \gamma).$$

Архитектура Критика. Задача Критика *Cr* – оценить разность между исходным изображением *C* и изображением, полученным Кодировщиком, т. е. определить изменения, вносимые в *C* встраиваемым секретным сообщением *M*. В ходе работы Критика выполняются следующие операции:

$$\alpha = Conv_{32\to 32}(Conv_{32\to 32}(Conv_{32\to 32}(C'))),$$

$$Cr(C') = Mean(Conv_{32\to 1}(\alpha)),$$

где $Mean(X)$ означает среднее арифметическое всех значений матрицы *X*.

Процесс Обучения. Будем использовать стохастический градиентный спуск для минимизации следующих функций потерь:

$$L_d = E_{XP_C}\left(\sum y_i \log y_i\right),$$

$$L_s = E_{XP_C}\frac{1}{3WH}\left\|(C - E(C,M))^2\right\|_2,$$

$$L_r = E_{XP_C}\left(Cr(E(C,M))\right),$$

где E_{XP_C} означает усреднение по всем элементам из используемого множества изображений (датасета), y_i – *i*-я компонента *M*. Целью обучения является минимизация $L_d + L_s + L_r$. Сеть Критик оптимизируем дополнительно, для чего минимизируем функцию:

$$L_c = E_{XP_C}\left(Cr(C)\right) - E_{XP_C}\left(Cr(E(C,M))\right).$$

В приведенных далее компьютерных экспериментах во время каждой итерации сопоставляется изображение *C* с секретным сообщением *M*, которое генерировалось случайным образом. Использовался оптимизационный алгоритм Adam [7], норма градиента уменьшалась до 0,25.

3. Результаты вычислительных экспериментов

3.1. Масштабирование данных. Первоначально для обучения использовался датасет, содержащий 1 500 изображений размерности 64×64 пикселя: 1 200 изображений использовались для обучения, 300 – для валидации. Далее датасет был увеличен до 75 000 изображений с целью проверки гипотезы о росте метрик при увеличении датасета. Из 75 000 изображений 55 000 использовались для обучения, 20 000 – для валидации. Обучение 30 эпох (шагов градиентного спуска) на таком датасете заняло около 150 часов на видеокарте NVidia Tesla K80. В результате обнаружено, что увеличение количества данных не приводит к увеличению метрик, и последующие эксперименты проводились с первоначальным датасетом – установлено, что его достаточно для обеспечения 100%-ной точности восстановления секретного сообщения для *M* для глубины кодирования *d*=1.

Масштабирование слоев. Сети Кодировщик и Декодировщик были расширены до 7 сверточных слоев, содержащих по 32 фильтра, обучение проводилось на 1 500 изображениях. В результате экспериментов установлено, что количество эпох, необходимых для сходимости сети – достижения Декодировщиком 100%-й точности восстановления *M* – выросло с 30 до 65, при этом прироста в метриках не наблюдалось. Более того, при добавлении обычных слоев без остаточных связей в сеть Критик наблюдается регресс сети и ухудшение метрик. Это объясняется тем, что добавление слоев смещает акцент Критика на более высокоуровневые признаки, в то время как два слоя выделяют более низкоуровневые признаки, такие как контраст, резкость и т. д., но именно по их изменению можно отследить,

что в изображение встроено секретное сообщение. Исходя из того, что масштабирование слоев не дает прироста, или даже вызывает регресс, полагаем, что количество слоев в исходной архитектуре достаточно для поставленной задачи стеганографии.

Масштабирование глубины кодирования. Одним из главных гиперпараметров рассматриваемой архитектуры является глубина кодирования d. Этот параметр определяет количество битов, встраиваемых в один пиксель изображения. Разумно предположить, что чем больше битов встраивается, тем сильнее меняется изображение, и тем легче Критик обнаруживает секретное сообщение M, и тем дольше работает Декодировщик, восстанавливая M из C', что проиллюстрировано в результатах вычислительных экспериментов, представленных в таблице 1. Точность Декодировщика вычислялась как среднее число правильно извлеченных бит сообщения M по всему датасету.

Таблица 1

Масштабирование глубины кодирования

Глубина кодирования	Количество эпох	Точность Декодировщика	Количество эффективных встроенных битов
1	35	100	0,99
4	80	0,9978	2,52

Заключение. Таким образом, в статье разработана генеративно-состязательная нейронная сеть, реализующая алгоритм встраивания секретного сообщения в изображение формата RGB. Проведены вычислительные эксперименты, иллюстрирующие работоспособность данной сети, в ходе которых наилучшие результаты получены при сравнительно небольшом (3–4) количестве сверточных слоев и размере датасета (1 500 изображений); установлено, что масштабирование глубины кодирования приводит к увеличению количества эффективно встраиваемой информации, но значительно увеличивает время работы Декодировщика и увеличивает вероятность обнаружения секрета Критиком.

Список литературы

1. Словарь основных терминов по криптологии / Ю. С. Харин [и др.].– Минск : БГУ, 2014. – 92 с.
2. Pevny, T. Steganalysis by subtractive pixel adjacency matrix / T. Pevny, P. Bas, J. Fridrich // Proc. of the 11th ACM Multimedia & Security Workshop. – Princeton, 2009. – P. 75–84.
3. Харин, Ю. С. Распознавание вкраплений в двоичную цепь Маркова / Ю. С. Харин, Е.В. Вечерко // Дискретная математика. – 2015. – Т. 27, В. 3. – С. 123–144.
4. Волошко, В. А. Стеганографическая емкость одномерного марковского контейнера / В. А. Волшоко // Дискретная математика. – 2016. – Т. 28, В. 1. – С. 19–43.
5. Goodfellow, I. J. Generative Adversarial Networks / I. J. Goodfellow [et al/]. – 2014.
6. He, K. Deep Residual Learning for Image Recognition / K. He, X. Zhang, S. Ren, J. Sun // 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). – 2016. – P. 770–778.
7. Kingma, D. Adam: A Method for Stochastic optimization / D. Kingma, J. Ba. – 2014.

УДК 004.421.6: 519.23

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ СТАТИСТИЧЕСКОГО ОЦЕНИВАНИЯ ЭНТРОПИИ

Р.А. КАПУСТО, В.Ю. ПАЛУХА
Белорусский государственный университет, г. Минск, Республика Беларусь

Введение. Одним из подходов к оценке качества генераторов случайных и псевдослучайных последовательностей является статистическое оценивание энтропии и сравнение полученной оценки с ожидаемым значением для равномерно распределенной случайной последовательности (РРСП). Данная работа посвящена сравнительному анализу методов статистического оценивания энтропии.

1. Обзор методов оценки энтропии. Пусть имеется случайная последовательность $\{x_i : i = 1,...,n\}$ из распределения вероятностей $\{p_k : k = 1,...,N\}$. Энтропия Шеннона данной последовательности вычисляется по формуле [1]:

$$H(P) = -\sum_{k=1}^{N} p_k \log p_k. \quad (1)$$

Поскольку истинные значения вероятностей неизвестны, мы можем лишь вычислить оценку энтропии последовательности. В работе рассмотрены несколько методов: подстановочный метод [2], метод Миллера-Мэдоу [3], байесовский метод [3], метод Грассбергера [4] и метод усадки Джеймса-Штейна [3].

Одним из подходов к статистическому оцениванию энтропии является построение частотных оценок вероятностей $\{\hat{p}_k\}$ и подстановка полученных оценок в функционал энтропии вместо истинных значений вероятностей $\{\hat{p}_k\}$. По подстановочному методу построение частотных оценок для вероятностей производится по следующим формулам:

$$\hat{p}_k = \frac{\nu_k}{n}, \quad \nu_k = \sum_{i=1}^{n} I\{x_i = \omega_k\}, \quad I\{x_i = \omega_k\} = \begin{cases} 1, x_i = \omega_k; \\ 0, x_i \neq \omega_k. \end{cases} \quad (2)$$

Методом Миллера-Мэдоу называют подстановочный метод, скорректированный с помощью константы,

$$\hat{H}_{MM} = \hat{H}_{plug-in} + \frac{\hat{N} - 1}{2n} \log e, \quad (3)$$

где $\hat{H}_{plug-in}$ – оценка, полученная подстановочным методом, $\hat{N}$ – оценка количества исходов с ненулевыми вероятностями.

Метод Байеса основан на корректировке оценок вероятностей и является еще одной модификацией подстановочного метода. Метод повторяет шаги плаг-ин оценки, только вместо формулы (2) используется следующая оценка:

$$\hat{p}_k^{Bayes} = \frac{\nu_k + a_k}{n + A}, \quad (4)$$

где a_k – поправочные коэффициенты, $A = \sum_{k=1}^{N} a_k$, $k = 1,...,N$.

Таким образом, оценка принимает следующий вид:

$$\hat{H}^{Bayes} = -\sum_{k=1}^{N} \hat{p}_k^{Bayes} \log \hat{p}_k^{Bayes}. \quad (5)$$

Метод Грассбергера также построен на основе подстановочного метода. Формула оценки следующая:

$$\hat{H}_G = \log n - \frac{1}{n}\sum_{k=1}^{N} v_k G_{v_k}, \quad G_k = \psi(k) + (-1)^k \int_0^1 \frac{x^{k-1}}{x+1} dx, \tag{6}$$

где $\psi(x) = \dfrac{d \ln \Gamma(x)}{dx}$ – дигамма функция, v_k вычисляется по формуле (2).

Усадка Джеймса-Штейна основана на усреднении двух абсолютно разных моделей: многомерной модели с низким смещением и высоким отклонением и модели более низкой размерности с большим смещением, но меньшей дисперсией. Интенсивность усреднения определяется относительным весом входящих в состав моделей. Коэффициент λ для выпуклой комбинации

$$\hat{p}_k^{Shrink} = \lambda t_k + (1-\lambda)\,\hat{p}_k^{ML} \tag{7}$$

является коэффициентом интенсивности усадки. Он принимает значения от 0 (нет усадки) до 1 (полная усадка). В формуле (7) $\hat{p}_k^{ML}$ – оценки вероятностей подстановочного метода, вычисленные по формулам (2), t_k – цель усадки.

Формула для вычисления коэффициента интенсивности усадки принимает вид

$$\hat{\lambda} = \frac{1 - \sum_{k=1}^{N} \left(\hat{p}_k^{ML}\right)^2}{(n-1)\sum_{k=1}^{N} \left(t_k - \hat{p}_k^{ML}\right)^2}. \tag{8}$$

Оценка энтропии по методу усадки Джеймса-Штейна производится по формуле

$$\hat{H}^{Shrink} = -\sum_{k=1}^{N} \hat{p}_k^{Shrink} \log \hat{p}_k^{Shrink}. \tag{9}$$

Для подстановочного метода в статье [5] приведено математическое ожидание оценки энтропии (используется натуральный логарифм):

$$E\left\{\hat{H}_{plug-in}\right\} = \ln n - e^{-\lambda} \sum_{k=1}^{+\infty} \frac{\ln(k+1)\lambda^k}{k!}, \quad \lambda = \frac{n}{N}. \tag{10}$$

Для этого метода вычислено математическое ожидание оценки энтропии в случае, если наблюдаемая последовательность является РРСП. Полученное значение использовалось в дальнейшем исследовании.

2. Сравнительный анализ. Анализ проводился на основе следующих показателей: среднее значение, среднеквадратическая ошибка, выборочная дисперсия. Данные принадлежали одному из двух алфавитов: бинарный (мощности 2) и байтовый (мощности 256). Для каждого алфавита получено по тысяче последовательностей из дискретного равномерного распределения размерами 10, 30, 50, 100, 300, 500, 1000, 3000 и 5000. В качестве генератора использовался стандартный генератор псевдослучайных символов языка программирования Python.

На первом этапе исследования были вычислены оценки энтропии рассмотренными методами, а также найдены средние значения указанных выше показателей. Далее цветами обозначены следующие методы: красный – подстановочный метод, желтый – метод Миллера-Мэдоу, зеленый – байесовская оценка, синий – метод Грассбергера, фиолетовый – метод усадки Джеймса-Штейна. На рисунках для построения графика выбраны наиболее информативные значения длин последовательностей (длины, для которых линии методов накладываются друг на друга, не включены).

На рисунке 1, где приведен график зависимости среднеквадратичного отклонения от длины последовательности для байтовой последовательности, показано, что значения, полученные по методу усадки Джеймса-Штейна, меньше среднего соответствующего параметра остальных методов. Это указывает на то, что значения энтропии, полученные методом усадки, ближе к эталонному значению энтропии. Смещение оценки энтропии, полученное по ме-

тоду Миллера-Мэдоу, меньше смещения соответствующей подстановочной оценки на всем рассматриваемом промежутке – как и требует построение метода.

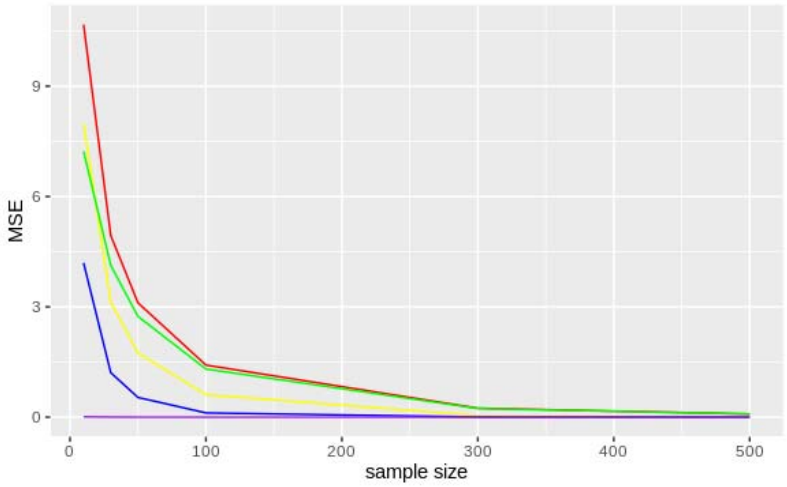


Рис. 1. Среднеквадратическое отклонение на последовательности байтов (равномерное распределение)

На рисунке 2 приведен аналогичный график для битовых последовательностей. Самое высокое среднеквадратическое отклонение у метода усадки Джеймса-Штейна.

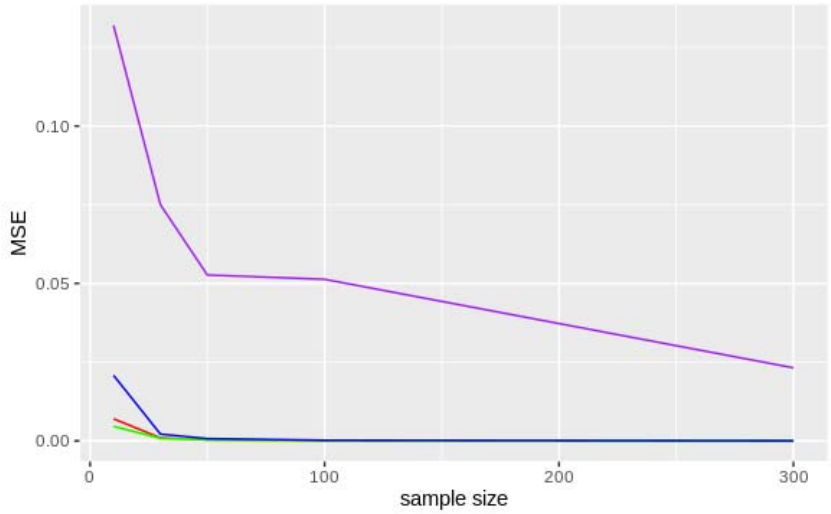


Рис. 2. Среднеквадратическое отклонение на последовательности битов (равномерное распределение)

На втором этапе исследования входные данные были модифицированы следующим образом: каждый десятый символ в последовательности битов был заменен нулевым, каждый сотый в последовательности байт – нулевым байтом. Целью описанного изменения было намеренно понизить энтропию входных данных, чтобы проследить реакцию методов на подобные изменения. Полагается, что чем больше отличаются оценки энтропии равномерно распределенных и модифицированных последовательностей, тем точнее мы сможем отличить последовательности таких генераторов в случае, когда нам неизвестно, продолжает генератор порождать равномерно распределенную случайную последовательность либо по каким-то причинам (поломка, подмена и т. п.) выходная последовательность не является равномерно распределенной. Для полученных последовательностей вычислены средние значения энтропии и другие показатели, как и для первого этапа исследования.

На рисунке 3 представлен график, отражающий разницу между средним значением энтропии для байтов на первом и втором этапе исследования. Для метода усадки Джеймса-Штейна разница наименьшая, что означает, что метод хуже всего откликается на понижение энтропии.

Рисунок 4 отражает аналогичную разницу для последовательностей битов. Так как на первом этапе метод усадки Джеймса-Штейна показал худший результат, этот метод не взят в рассмотрение на рисунке 4.

Метод Грассбергера имеет меньшую разницу из всех методов. Остальные методы имеют приблизительно одинаковые показатели.

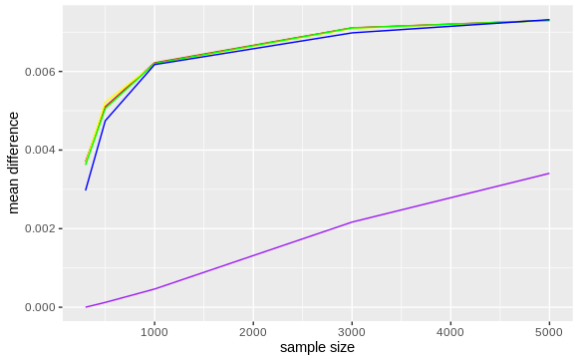


Рис. 3. Разность среднего значения энтропии на последовательности байтов

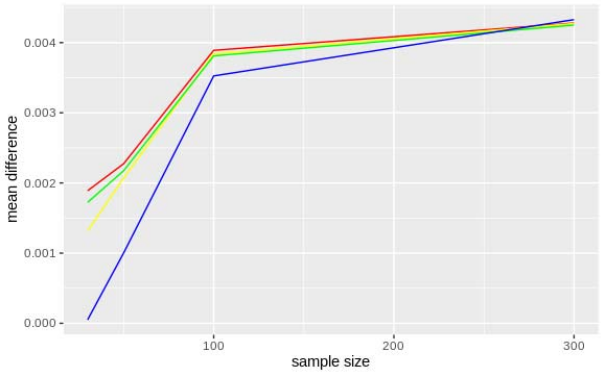


Рис. 4. Разность среднего значения энтропии на последовательности битов

Заключение. По результатам проведенных исследований можно сделать следующие выводы о методах оценки энтропии Шеннона.

1. Плаг-ин оценка: стабильна, средние относительно других методов показатели смещения и дисперсии. Базовый метод.
2. Метод Миллера-Мэдоу: показатели смещения лучше, но уступает в дисперсии плаг-ин оценке.
3. Байесовская оценка: результаты, как и у плаг-ин оценки.
4. Метод Грассбергера: малое отклонение, но большая дисперсия. Метод хуже других проявил себя на втором этапе исследований по распознаванию модифицированных последовательностей.
5. Метод усадки Джеймса-Штейна: плохие результаты для битовых последовательностей. Так как на втором этапе исследований метод плохо себя проявил, его применимость остается под вопросом.

Список литературы

1. Shannon, C. E. A mathematical theory of communication / C. E. Shannon // Bell. System Tech. – 1948. – J. 21. – P. 379–423.

2. Башарин, Г. П. О статистической оценке энтропии последовательности независимых случайных величин / Г. П. Башарин // Теория вероятн. и ее примен. – 1959. – Т. 4, вып. 3. – С. 361–364.

3. Hausser, J. Entropy Interference and the James-Stein Estimator, With Application to Nonlinear Gene Association Networks / J. Hausser, K. Strimmer // Journal of Machine Learning Research. – 2009. – J. 10. – P. 1469–1484.

4. Grassberger, P. Entropy Estimates from Insufficient Sampling [Electronic resource] / P. Grassberger. – Режим доступа : https://arxiv.org/pdf/physics/0307138.pdf. – Дата доступа : 31.03.2021.

5. Палуха, В. Ю. Статистические тесты на основе оценок энтропии для проверки гипотез о равномерном распределении случайной последовательности / В. Ю. Палуха // Весці НАН Беларусі. Серыя фізіка-матэматычных навук. – 2017. – № 1. – С. 79–88.

ЗАОЧНЫЕ ДОКЛАДЫ

УДК 002.6; 004.7; 004.722

ПРОЕКТИРОВАНИЕ МНОГОСЛОЙНОЙ ОТКАЗОУСТОЙЧИВОЙ СИСТЕМЫ ОНЛАЙН ОБУЧЕНИЯ В УСЛОВИЯХ ПОВЫШЕННОЙ НАГРУЗКИ

В.П. КОЧИН, А.В. ЖЕРЕЛО
Белорусский государственный университет, г. Минск, Республика Беларусь

В настоящее время в условиях короновирусной инфекции очень остро стоит вопрос создания отказоустойчивой системы онлайн обучения в условиях повышенной нагрузки [1]. При проектировании такой системы необходимо учитывать следующие факторы: большие количество одновременно работающих клиентов, обеспечение отказоустойчивости системы с учетом возможных кибератак. Для решения этой задачи целесообразно использовать технологии виртуализации не только отдельных ресурсов, но и виртуализации сетевой инфраструктуры учреждений [2, 3]

Для построения надежной системы необходимо учесть особенности архитектуры среды, на которой данная система базируется. В случае современной облачной среды основными компонентами телекоммуникационной архитектуры являются [4, 5]:

Data plane (плоскость данных), control plane (плоскость управления) и management plane (плоскость администрирования). Data plane определяет ту часть сетевой инфраструктуры, через которую передаются пользовательские пакеты. Это теоретический термин, используемый для концептуализации потока пакетов данных через сетевую инфраструктуру.

Control plane является частью сети, которая переносит сигнальный трафик и отвечает за маршрутизацию. Пакеты управления или исходят, или предназначены для маршрутизатора. Функции плоскости управления включают в себя настройку системы и управление.

Management plane – это элементы системы, которые осуществляют конфигурирование, мониторинг и управление всеми подуровнями сетевой инфраструктуры. Management plane, которая несет административный трафик, считается подмножеством control plane.

В традиционных сетях все три плоскости реализованы в маршрутизаторах и коммутаторах аппаратно (как правило, в виде прошивки устройства).

В программно-определяемой сети (SDN) производится разделение плоскостей данных и управления. Это позволяет извлечь функции плоскости управления из сетевого оборудования и реализовать их в виде отдельного программного обеспечения, что позволяет организовать программируемый доступ и, как следствие, делает администрирование сети гораздо более гибким.

Перемещение плоскости управления в программное обеспечение предоставляет возможность организовать динамический доступ элементам сетевой инфраструктуры на всех уровнях и обеспечить их «прозрачное» администрирование. Таким образом, администратор может формировать трафик с централизованной консоли управления, не взаимодействуя с отдельными коммутаторами и маршрутизаторами. При необходимости он так же может изменять правила поведения любого сетевого устройства, например, назначать и отменять приоритеты определенным потокам данных, блокировать определенные типы пакетов используя детальный уровень контроля [5].

Для организации доступа к ресурсам виртуальной сети такое разделение позволяет получить дополнительные преимущества с точки зрения организации устойчивого и надежного функционирования виртуальной сети в целом. Подход с разделением плоскости данных и управления позволяет создать логически изолированные зоны, или так называемые «песочницы», которые в нашем случае представляют взаимодействующие локальные сетевые сегменты, объединяющие между собой узконаправленные по своей функциональности сервисы. Это позволяет воспользоваться преимуществами микросервисной архитектуры для организации блочного подхода к реализации «песочницы» [6].

Определим три типа виртуальных сетей: внешние, внутренние и приватные. В нашем случае, внешние сети – это сети, имеющие выход в интернет. Внутренние виртуальные се-

ти – это сети, к которым могут подключаться только виртуальные интерфейсы виртуальных машин ОС. Приватные сети, это сети, к которым могут подключаться интерфейсы виртуальных машин и интерфейсы хостовой ОС, ведущие в частную корпоративную сеть.

Используем предложенное разбиение будет в последствии использовано для организации аутентификации и авторизации.

Напомним, что при построении системы необходимо решить следующие поставленные задачи:

- обеспечить мобильность пользователей.
- снизить затраты на развитие и решение проблем надежности, производительности и безопасности.
- обеспечить единообразный доступ как к внутренним ресурсам сети учреждения, так и к облачным.

На данный момент вопрос о мобильности пользователей системы решается, можно сказать, естественным образом. Широкая распространенность средств доступа к сети Интернет позволяет (с пользовательской точки зрения) реализовать набор порталов и интерфейсов, обеспечивающих доступ к ресурсам облачной инфраструктуры, тогда основной задачей на линии взаимодействия «пользователь» – «сервис» является задача защиты канала, которая решается за счет шифрования и прочих средств обеспечения безопасности канала (например, двухсторонняя идентификация участников обмена).

С технической точки зрения, основной задачей для облачной инфраструктуры является обеспечение достаточного количества ресурсов для поддержания необходимого количества пользователей и реализация механизмов масштабирования, для предупреждения возможного скачкообразного роста потребителей ресурсов. Эта задача может разделяется на два основных аспекта, технический и организационный, и может быть решена централизованно без привлечения специалистов учреждений, которым оказываются услуги по доступу в облако [5, 6]. В случае роста технических требований к ресурсам (процессорные мощности, объем памяти и т. д.) в силу абстрактности уровней архитектуры, проблему можно решить, арендовав необходимые мощности в коммерческих облаках, либо за счет развертывания дополнительных вычислительных ресурсов в уже используемых ЦОД учреждений. Необходимо отметить, что в ряде случаев аренда может быть предпочтительным решением, т.к. она позволяет оперативно задействовать дополнительные мощности и единовременно требует меньших вложений. Аренда мощностей также является приемлемым решением при решении нарастить мощности уже используемых ЦОД, т.к. срок, в течении которого необходимо предоставить дополнительные ресурсы пользователям, как правило, значительно короче, чем работы по расширению ресурсной базы того или иного ЦОД, и тем более, создание нового ЦОД. Иногда проблемы возникают из-за ограничений используемых программных решений, например, ограничение на количество пользовательских подключений или на количество и скорость транзакций при обращении к базам данных. В этом случае проблемы могут быть решены организационно за счет предварительного проектирования и создания используемых образов сервисов, которые в последствии будут оперативно развернуты в нужных точках облачной инфраструктуры.

Особое внимание обращает на себя задача по обеспечению единообразного доступа к внутренним и облачным ресурсам сети учреждения. Это связано, прежде всего, с децентрализованным характером развития ЛВС учреждений и, как итог, различными регламентами использования сетей. Преобразование всей инфраструктуры и разработка единого регламента, регулирующего все аспекты функционирования сетей, требует существенных затрат, а в ряде моментов, является невозможным из-за специфических особенностей некоторых учреждений. Решением задачи единообразного доступа является переход от LAN и VLAN к идее VXLAN. Тогда подключение пользователя производится к облачному отображению локальной сети учреждения. В свою очередь, сеть учреждения представляется как набор физических и логических сегментов, где логические сегменты могут располагаться в некотором облаке, а взаимодействие между сегментами обеспечивается за счет использования услуги VPNaaS (VPN as a Service), осуществляющей туннелирование локального трафика, его шифрование и идентификацию каналов подключения. Т.к. эта часть технически основана на использовании образов используемых сервисов, такой подход повышает надежность использования ЛВС учреждения, т.к. позволяет

с минимальными затратами менять расположение решений, требующих определенных вычислительных мощностей, не изменяя при этом структуры сети учреждения [2, 3].

Таким образом, для создания многослойной отказоустойчивой системы учреждения необходимо выполнить следующие этапы:

1. определить потребности в оказываемых услугах и необходимых для их развертывания ресурсах;

2. определить текущую топологию ЛВС учреждения и спроектировать и требования к ее интеграции в создаваемую облачную инфраструктуру;

3. определить пользователей ресурсов и их группы. Определить соответствующие права и внести данную информацию в Active Directory.

4. На базе полученной информации организовать изолированный виртуальный сетевой сегмент, создав в облаке проект, определяющий внешнюю сеть, в которой будут располагаться требуемые пользовательские сервисы, и организовать взаимодействие этой сети с внутренней сетью, содержащей промежуточный сервер авторизации, или организовать новую внутреннюю сеть, соединяющуюся с приватной сетью, в случае необходимости.

На рисунке 1 приведен многослойной структуры системы онлайн обучения в Белорусском государственном университете.

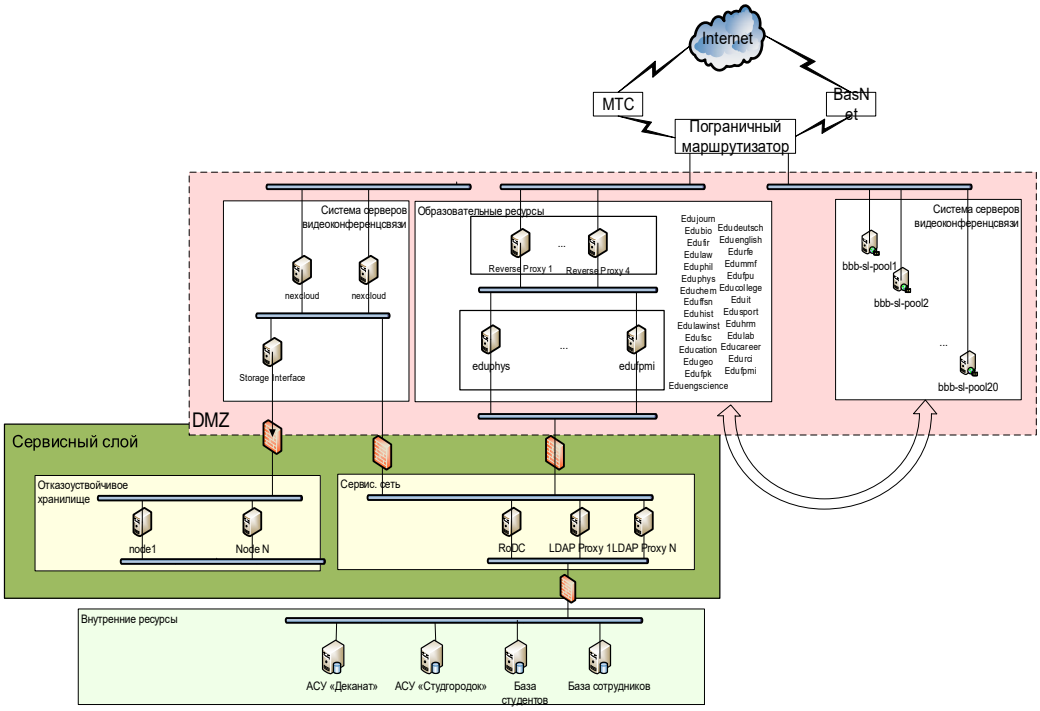


Рис. 1. Архитектура многослойной структуры системы онлайн облучения в БГУ

Применение такого подхода позволило обеспечить повышенный уровень безопасность и целостность данных при атаке на образовательные ресурсы БГУ, а также обеспечить быстрое восстановление работоспособности образовательных ресурсов после распределенной ddos-атаки.

Список литературы

1. Король, А. Д. Дистанция в образовании: от методологии к практике / А. Д. Король, Ю. И. Воротницкий, В. П. Кочин // Наука и инновации. – 2020. – № 6 (208). – С. 22–29.

2. Кочин, В. П. Виртуализация сетевой инфраструктуры учреждений образования / В.П. Кочин, Ю. И. Воротницкий, А. В. Жерело // Цифровая трансформация. – 2020. – № 1(10). – С. 51–56.

3. Кочин, В. П. Виртуализация сетевой инфраструктуры Белорусского государственного университета / В. П. Кочин, А. В. Жерело // Вестник компьютерных и информационных технологий. – 2020. – № 8. – С. 45–52.

4. Официальный сайт OpenStack. [Электронный ресурс]. – Режим доступа : https://www.openstack.org/. – Дата доступа : 20.03.2021.

5. Goransson, P. Software Defined Networks. A Comprehensive Approach. Second Edition / P. Goransson, C. Black, T. Culver // Elsevier. – 2017. – 409 p.

6. Subramanian, S. Software-Defined Networking (SDN) with OpenStack / S. Subramanian, S. Voruganti. – Packt Publishing, 2016. – 216 p.

УДК 004.056.5

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТА ИНФОРМАЦИИ ОБЛАЧНЫХ РЕСУРСОВ

В.П. КОЧИН, А.В. ШАНЦОВ
Белорусский государственный университет, г. Минск, Республика Беларусь

Введение. На сегодняшний день облачные технологии получили широкую популярность: экономичность, легкость развертывания, многопользовательская архитектура – все это способствует быстрому распространению облаков. Экономичность облаков делает их особенно популярными для хранения информации. Компании также используют публичные облака для проектов, требующих временных вычислений, из-за подхода к оплате «плати за использование». Они могут использовать публичные облака вместо того, чтобы настраивать собственную внутреннюю инфраструктуру только лишь для частичного или временного использования. Но облачная инфраструктура также представляет повышенные риски информационной безопасности и ограниченную возможность управления ресурсами. В этом и заключаются главные проблемы облачных вычислений – защита информации и доверие пользователей по отношению к облачным провайдерам [1]. Риски информационной безопасности облачных вычислений усугубляются тем фактом, что защита менее защищенной части облака определяет общий уровень защищенности [2]. Так, например, успешная DDoS-атака на облачный балансировщик нагрузки может заблокировать доступ ко всему облаку, несмотря на то, что внутри облако будет работать устойчиво. Аналогично SQL-инъекция, прошедшая через сервер приложений, предоставит доступ к данным системы, не зависимо от правил разграничения доступа и т. д.

Угрозы информационной безопасности облачных ресурсов. Для защиты от угроз информационной безопасности система защиты информации (далее – СЗИ) облачных ресурсов должна носить комплексный характер и обеспечивать защиту от угроз технического и физического характера, а также должна соответствовать юридическим требованиям. Комплексная СЗИ позволит в равной мере исключить угрозы для облачных информационных ресурсов, обусловленных различными факторами. За основу при построении комплексной СЗИ облачных ресурсов можно взять СЗИ традиционных вычислений. Однако облачные вычисления, из-за своих особенностей [3], будут оказывать существенное влияние на архитектуру СЗИ. Особенно сильное влияние облачные вычисления оказывают на защиту от технических угроз и на подтверждение соответствия юридическим требованиям [4].

Угрозы технического характера. На высоком уровне можно выделить следующие виды технических угроз:

– угрозы атак на систему виртуализации;
– угрозы атак на клиентов облака;
– угрозы традиционных атак на программное обеспечение;
– угрозы атак на инфраструктуру облака; комплексные угрозы.

Рассмотрим подробнее каждый вид технических угроз:

1. Угрозы атак на систему виртуализации. Поскольку платформой для компонентов облака является виртуальная среда, то атаки на систему виртуализации угрожают всему облаку в целом. Среди угроз виртуализации можно выделить:

1.1. Угрозы гипервизору. Ключевым элементом виртуальной системы является гипервизор, который обеспечивает разделение ресурсов аппаратной платформы между виртуальными машинами (далее – ВМ). Вмешательство в работу гипервизора может привести к тому, что одна ВМ может получить доступ к ресурсам другой, перехватывать ее сетевой трафик, отбирать ее физические ресурсы и т. д.

1.2. Угрозы миграции ВМ. ВМ представляет собой по сути файл, который может быть запущен на исполнение в разных узлах облака. В системах управления облачными ресурсами предусмотрены механизмы переноса ВМ с одного узла на другой. Однако файл ВМ можно перехватить и похитить, с последующим запуском его за пределами облака.

1.3. Угрозы системам управления облака. Огромное количество ВМ, особенно в публичных облаках, требуют таких систем управления, которые могли бы надежно контролировать создание, перенос и утилизацию ВМ. Вмешательство в системы управления может

привести к появлению ВМ «невидимок», блокирование одних машин и подстановка в слои облака неавторизованных элементов.

1.4. Угрозы заражения бездействующих ВМ. Выключенная ВМ подвергается опасности заражения из-за невозможности запустить на ней защитное программное обеспечение.

1.5. Угрозы отзыва лицензии. На сегодняшний день данная угроза носит лишь теоретический характер, однако санкционная политика, в том числе и в отношении Республики Беларусь, делает возможным и такой сценарий. Угроза заключается в отзыве лицензий на коммерческие продукты виртуализации для центров обработки данных (далее – ЦОД), являющихся государственной формой собственности или обслуживающих государственные организации. В случае реализации данной угрозы, ЦОД лишается поддержки по обновлению и регулярному внесению исправлений в средства системы виртуализации, что влечет за собой возникновению новых угроз информационной безопасности для облачных ресурсов. В качестве альтернативы можно рассмотреть использование средств, не требующих лицензий, однако их использование связано со значительно большими затратами на развертывание, настройку и поддержку по сравнению с коммерческими.

2. Угроза атаки на клиентов. Данный вид угрозы можно условно разделить на несколько категорий. К первой категории можно отнести атаки, широко распространенные в веб-среде. Данные атаки также актуальны и для облака, поскольку ряд облачных услуг подразумевает подключение клиентов к облачным сервисам с помощью веб-браузеров. К данной категории относят такие атаки как межсайтовый скриптинг, перехваты веб-сессий, воровство паролей, «человек посредине» и другие. Облачные вычисления повышают актуальность данной угрозы, так как при отсутствии должной изоляции между клиентами облака, успешная реализация атаки на одного из клиентов может привести к значительному расширению плоскости атаки и подвергнуть риску все облако в целом. Отдельно можно выделить угрозы утечки информации при перераспределении ресурсов облака. Облачные ресурсы имеют динамичный характер и могут при необходимости освобождать или запрашивать новые ресурсы. В этом случае должно быть гарантировано, что при перераспределении ресурсов новый пользователь не сможет восстановить данные предыдущего пользователя. Также должна быть гарантирована защита энергозависимой памяти от несанкционированного мониторинга, который может привести к раскрытию информации пользователей облака.

3. Угрозы традиционных атак на программное обеспечение (далее – ПО). Угрозы, связанные с традиционными атаками на ПО в зависимости от модели предоставляемых облаком услуг, могут быть отнесены как к атакам на клиентов облака, так и как отдельный вид угроз для облачного провайдера. К данным угрозам можно отнести атаки на операционные системы и приложения, разворачиваемые на облачных платформах. Как правило, это атаки, связанные с использованием уязвимостей в ПО, атаки с использованием вредоносного ПО и другие виды широко распространенных атак.

4. Угрозы атак на инфраструктуру облака. Защита инфраструктуры – один из ключевых аспектов обеспечения безопасности в традиционных вычислениях. Подход по защите инфраструктуры облачных ресурсов заимствован из традиционных вычислений, однако, при его использовании, необходимо учитывать особенности, вносимые облачными вычислениями. Например, при развертывании на ВМ в облаке межсетевых экранов, прокси-серверов и других средств безопасности следует учитывать, что ВМ, в основном, не столь производительны как аппаратные решения и могут стать «бутылочным горлом» в создаваемой сети. При использовании облачных вычислений периметр сети размывается, что значительно затрудняет защиту с помощью традиционных межсетевых экранов. Традиционные системы обнаружения вторжений, при их развертывании в облаке, не смогут отслеживать трафик, проходящий между ВМ, развернутыми на одной аппаратной платформе [5].

5. Комплексные угрозы. Комплексные угрозы, в контексте рассмотрения технических угроз облачным вычислениям, можно рассматривать как совокупность вышеперечисленных технических угроз облачным вычислениям.

Физические угрозы. Характер физических угроз связан с защитой ЦОД и по своей сути ничем не отличается от того, какие услуги предоставляет ЦОД: облачные или традиционные. К основным физическим угрозам можно отнести угрозы техногенного характера и угрозы физического воздействия.

К угрозам техногенного характера относятся стихийные бедствия, пожары, затопления и т. д. к угрозам физического воздействия можно отнести хищение, уничтожение оборудования, несанкционированный доступ к оборудованию, выход из строя системы электроснабжения, нарушение условий кондиционирования и другие [6].

Соответствие юридическим требованиям. Подтверждение соответствия юридическим требованиям, как правило связано с подтверждением соответствия развернутого облачного ресурса регулирующим техническим нормативным правовым актам (далее – ТНПА) в области защиты информации, а также ТНПА, регулирующим обработку персональных и конфиденциальных данных. Основными проблемами, с одной стороны, может быть отсутствие нормативно-правовой базы, регулирующей облачные вычисления и необходимость аттестации (сертификации) облачных ресурсов на соответствие ТНПА, не учитывающих специфику облачных вычислений. С другой стороны, проблемы могут заключаться в сложности либо невозможности выполнения ряда требований ТНПА, например, обработка персональных и конфиденциальных данных только в пределах территории государства для международных облачных провайдеров, противоречия в распространяемых юрисдикциях при обработке данных на территории нескольких государств и другие [7].

Комплексная СЗИ. Существует большое разнообразие моделей развертывания облака и моделей предоставляемых облачных услуг. Архитектуры облачных ресурсов носят индивидуальный характер. Для каждого отдельно взятого облака СЗИ нужно строить также индивидуально. Тем не менее, СЗИ должна носить комплексный характер и, как правило, должна включать подсистему централизованного управления средствами защиты информации; подсистему обнаружения и предотвращения вторжений; подсистему антивирусной защиты; подсистему криптографической защиты информации; подсистему межсетевого экранирования; подсистему контроля, управления и разграничения доступа (как техническую, так и физическую); подсистему мониторинга и управления событиями; подсистему контроля целостности информации и приложений; подсистему резервного копирования и восстановления данных; подсистему видеонаблюдения и охранно-пожарной сигнализации. В отдельности каждые из этих защитных механизмов уже созданы и широко представлены на рынке. Однако, для построения комплексной СЗИ необходимо на этапе создания облачной платформы решить задачу по интеграции средств безопасности в единую комплексную систему. Дополнительно, при выборе средств безопасности, необходимо оценить риски, связанные с использованием лицензируемых коммерческих продуктов. Кроме того, облачный ресурс должен быть подвергнут аудиту в целях подтверждения соответствия ТНПА и получения необходимых аттестатов (сертификатов).

Заключение. СЗИ должна учитывать наличие угроз различного характера. Построение самой продвинутой технической СЗИ может быть полностью обесценено при отсутствии должной защиты от физических угроз в случаях техногенных аварий или физического воздействия на аппаратные платформы. СЗИ, обеспечивающая надежную защиту от технических и физических угроз, может быть лишена всякого смысла если она не будет соответствовать требованиям законодательства, и, как следствие, такой облачный ресурс не будет аттестован (сертифицирован). Таким образом, СЗИ облачных ресурсов должна носить комплексный характер. Лишь комплексная СЗИ способна обеспечить надежную защиту информационных ресурсов, обрабатываемых в облаке, и подтвердить соответствие облачного ресурса регулирующим ТНПА.

Список литературы

1. Ивонин, П. В. Безопасность облака в деталях. Безопасность информационных технологий / П. В. Ивонин. – 2013. – № 2 (20). – С. 37–40.

2. Информационный ресурс Anti-malware [Электронный ресурс]. – Режим доступа : https://www.anti-malware.ru/node/2333. – Дата доступа : 09.04.2021.

3. National Institute of Standards and Technology, Special Publication 500-292 «Cloud Computing Reference Architecture».

4. Информационный ресурс Kaspersky [Электронный ресурс] – Режим доступа : https://www.kaspersky.ru/resource-center/definitions/what-is-cloud-security. – Дата доступа : 12.04.2021.

5. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing.

6. Корелин, И. А. Жизнеобеспечение центра обработки данных: защита и риски. Физическая защищенность : мат-лы XVI Всеросс. науч.-практ. конф. / И. А. Корелин, Т. М. Мкртчян. – УрГУ, 2017.

7. Шекель, Н. В. Юридические аспекты использования облачных технологий / Н. В. Шекель // Журнал международного права и международных отношений. – 2014. – № 4 (71). – С. 3–7.

УДК 621.3.085.345

ВЛИЯНИЕ РАЗМЕРА ОДИНОЧНЫХ ЭЛЕМЕНТОВ, ОБРАЗУЮЩИХ КОНСТРУКЦИЮ ЭКРАНА ЭМИ, НА ЕЕ ЭКРАНИРУЮЩИЕ СВОЙСТВА

С.Э. САВАНОВИЧ
Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Возможность обнаружения и идентификации наземных объектов обеспечивается посредством электромагнитного канала (ЭМК) утечки информации, формируемого излучениями средств технической разведки (СТР) и излучениями, отраженными наземными объектами и окружающей средой, на фоне которой они находятся, принятыми антенной системой СТР [1]. Обработка принятых излучений по определенному алгоритму позволяет сопоставить их интенсивности и получить информацию о наличии наземных объектов в зоне действия СТР, а также их идентифицировать, в соответствие с чем, проблема противодействия получению таких сведений является весьма актуальной задачей [2].

Известно [3], что решение задачи защиты информации о наземных объектах осуществляется с помощью методов, основанных на снижении различий в интенсивностях ЭМИ, отраженных наземными объектами и окружающей средой, или снижении интенсивности отраженных объектами излучений до уровня, который ниже или сравним с порогом их обнаружения СТР в диапазоне частот 2–12 ГГц. Реализация таких методов обеспечивается применением средств скрытия, позволяющих изменить отражающую способность объектов по отношению к окружающей среде; использованием устройств, обеспечивающих изменение направленности излучений, отраженных объектами; применением «малоотражающих» форм, позволяющих снизить интенсивность отраженных излучений; использованием конструкций экранов ЭМИ, обеспечивающих изменение отражающих свойств объектов [4].

Вышеперечисленные средства противодействия перехвату информации по ЭМК не обеспечивают достаточный уровень снижения интенсивности ЭМИ, отраженных от поверхности объектов, в случае изменения погодных условий, сложны при их технической реализации, и характеризуется высокой стоимостью. Основным средством, обеспечивающим защиту информации об объектах в диапазоне частот функционирования СТР, является применение конструкций экранов ЭМИ, наносимых на их поверхность [5]. Практически все материалы, применяемые в конструкциях экранов ЭМИ, являются неоднородными по структуре композиционными материалами, полученными в результате синтеза компонентов с определенными электрофизическими параметрами. Это обусловлено необходимостью соблюдения требований, выполнение которых позволяет снизить интенсивность излучений, отраженных от поверхности защищаемых объектов, до требуемого уровня в широком диапазоне частот: излучения СТР должны проникать в материал с минимальным отражением на границе сред «свободное пространство – поверхность экрана ЭМИ», излучения должны поглотиться в материале экрана, сложиться в противофазе с излучениями СТР, или рассеяться на неоднородностях материала экрана [6]. Независимо от принципа действия к конструкциям экранов ЭМИ предъявляют ряд требований, основными из них являются: значения коэффициентов отражения и передачи в диапазоне частот функционирования СТР, по возможности минимальный вес; способность работать в широком интервале температурных режимов; надежность и долговечность. Основными недостатками существующих конструкций экранов ЭМИ являются сложность в их изготовлении, узкий диапазон рабочих частот, высокая стоимость.

Перспективным направлением в разработке конструкций экранов ЭМИ представляется применение влагосодержащего керамзита. В работах [7, 8] установлено, что размер фракций (размер пор) керамзита определяет рабочий диапазон частот конструкций экранов, выполненных на его основе, а мнимая составляющая диэлектрической проницаемости (ε'') и влагосодержание керамзита оказывают влияние на значения коэффициента отражения таких экранов. Показано, что применение керамзита с размером фракций 1…2 мм в кон-

струкции экрана ЭМИ позволяет снизить ее значения коэффициента отражения на частотах 7,7–17,0 ГГц, керамзита с размером фракций 10…20 мм – на частотах 1,0–7,7 ГГц.

Предложена конструкция экрана ЭМИ в виде одиночных элементов (площадок), выполненных на основе керамзита с размерами фракций 1…2 и 10…20 мм, что позволит расширить диапазон рабочих частот экрана. При этом значения коэффициента отражения ЭМИ такой конструкции будут определяться размерами одиночных элементов, взаимным расположением площадок с керамзитом, ε'' растворов, вводимых в его поры, толщиной конструкции. Таким образом, целью данной работы являлось исследование влияния размера одиночных элементов, образующих конструкцию экрана ЭМИ, на ее экранирующие свойства в диапазоне частот 2–12 ГГц.

Для проведения исследования подготовлены и стабилизированы по массе образцы керамзита с размерами фракций 1…4 и 10…20 мм. Для пропитки керамзита применялись растворы, выполненные на основе хлорида натрия (NaCl) и натриевой соли карбоксиметилцеллюлозы (Na-КМЦ). Концентрация NaCl и Na-КМЦ в водном растворе, вводимом в поры керамзита с размером фракций 1…2 мм, составляла 20 и 2 %, с размером фракций 10…20 мм – 20 и 4 % соответственно. Температура дистиллированной воды при приготовлении растворов варьировалась в пределах 48…50 °С. Влагосодержание керамзита с размерами фракций 1…4 и 10…20 мм, содержащего приготовленные растворы, составляло 36…39 и 38…40 % соответственно. Введение в поры керамзита приготовленных растворов осуществлялось методом иммерсионного смачивания при атмосферном давлении 101,3 кПа и температуре окружающей среды 20 ± 3 °С. Время пропитки керамзита приготовленными растворами составляло 48^{+1} ч. Для проведения исследования изготовлены две конструкции экрана ЭМИ (далее по тексту – конструкция №1 и №2) в виде листов толщиной 10 ≈ 12 мм на основе влагосодержащего керамзита с размерами фракций 1…2 и 10…20 мм и полиуретановой мастики (рис. 1). При формировании конструкций № 1 и 2 нижний слой экрана ЭМИ, выполненный на основе стекловолокна и полиуретановой мастики, разбивался на площадки, на которых размещался подготовленный керамзит, с последующей его герметизацией вторым слоем мастики. Размеры одиночных элементов конструкции экрана ЭМИ рассчитывались по формуле

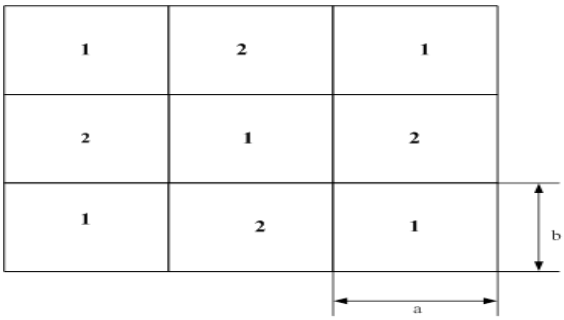


Рис. 1. Схема размещения керамзита на одиночных элементах конструкций № 1 и 2: *1* – размер фракций 1…2 мм, *2* – размер фракций 10 – 20 мм

$$a + b \approx \frac{2\lambda}{\sqrt{\varepsilon}},$$

где a и b размеры одиночных элементов, λ – рабочая длина волны конструкции экрана ЭМИ, ε – относительная диэлектрическая проницаемость материала, из которого изготовлена внешняя поверхность экрана [9]. Размеры элементов рассчитывались на частоты 3 и 7 ГГц и составляли для конструкции №1 – 60×40 мм, №2 – 30×20 мм. Линейный размер конструкции экрана ЭМИ составлял 400×320 мм.

Для измерения значений коэффициентов отражения ЭМИ конструкции № 1 и 2 в диапазоне частот 2–12 ГГц использовался панорамный измеритель коэффициентов передачи и отражения SNA 0,01–18, работающий по принципу раздельного выделения и непосредственного детектирования уровней падающей и отраженной волн, и антенны П6–23М. При измерении значений коэффициентов отражения ЭМИ конструкции № 1 и 2 размещалась на металлической подложке, которая имитировала поверхность наземной техники. Измерения проводились по методике, приведенной в [10].

На основании анализа полученных результатов установлено, что уменьшение размеров одиночных элементов в два раза приводит к увеличению значений коэффициента отражения ЭМИ конструкции №2 в диапазоне частот 1–17 ГГц (рис. 2, 3).

Разница в значениях коэффициентов отражения ЭМИ для конструкций №1 и 2 в рассматриваемом диапазоне частот составляла до 10 дБ.

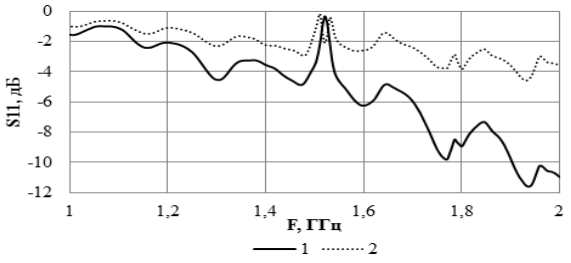


Рис. 2. Частотные зависимости (диапазон частот 1–2 ГГц) значений коэффициентов отражения конструкций № 1 и 2, выполненных на основе влагосодержащего керамзита, размещенных на металлической подложке:
1 – конструкция № 1; *2* – конструкция № 2

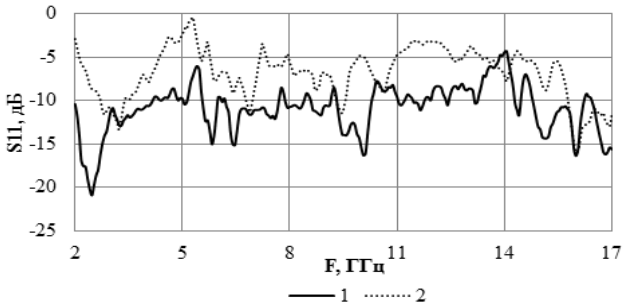


Рис. 3. Частотные зависимости (диапазон частот 2–17 ГГц) значений коэффициентов отражения конструкций №1 и 2, выполненных на основе влагосодержащего керамзита, размещенных на металлической подложке:
1 – конструкция № 1; *2* – конструкция № 2

Показано, что применение в конструкции экрана ЭМИ влагосодержащего керамзита с размерами фракций 1…2 и 10…20 мм, выполненной в виде одиночных элементов с размерами площадок 60×40 мм, приводит к расширению ее рабочего диапазона частот и обеспечивает снижение значений коэффициента отражения на частотах 1,8–13,2 ГГц до уровня не ниже -10…-8 дБ.

Можно предположить, что в случае выполнения конструкции экрана ЭМИ в виде одиночных элементов, каждый из таких элементов обеспечивает снижение значений коэффициента отражения за счет поглощения, интерференции и дифракции излучений на частотах, соразмерных и кратных размерам площадок. Это подтверждается расширением диапазона рабочих частот конструкции №1 при увеличении размера одиночных элементов с 30×20 до 60×40 мм. Что показывает перспективность применения такой конструкции в целях защиты информации о наземных объектах в диапазоне частот 2–12 ГГц.

Список литературы

1 Меньшаков, Ю. К. Виды и средства иностранных технических разведок : учеб. пособие / Ю. К. Меньшаков ; под ред. М. П. Сычева. – М. : Изд-во МГТУ им. Н.Э Баумана, 2009. – 656 с., ил.

2. Модели технических разведок и угроз безопасности информации. Коллективная монография / под ред. Е. М. Сухарева. – М. : Радиотехника, 2003.– 144 с.

3. Лыньков, Л. М. Поглотители электромагнитного излучения. Применение в вооруженных силах : моногр. / Л. М. Лыньков [и др.]. – М. : Бестпринт, 2006. – 228 с.

4. Алексеев, А. Г. Физические основы технологии Stealth / А. Г. Алексеев, Е. А. Штагер, С. В. Козырев. – СПб. : ВВМ, 2007. – 284 с.

5. Львова, Л. А. Радиолокационная заметность летательных аппаратов / Л. А. Львова. – Снежинск : Изд-во РФЯЦ – ВНИИТФ, 2003. – 232 с.

6. Филин, С. А. Средства снижения заметности (по патентным материалам) / С. А. Филин, Л. А. Малохина. – М. : ИНИЦ Роспатента, 2003. – 215 с.

7. Саванович, С. Э. Влияние вязкости водного раствора хлорида натрия, введенного в поры керамзита, на его радиопоглощающие свойства / С .Э. Саванович, Т. В. Борботько // Весці Нац. акадэміі навук Беларусі. Серыя фізіка-тэхнічных навук. – 2016. – № 2. – С. 115–119.

8. Саванович, С. Э. Влияние влагосодержания керамзита на значения коэффициента отражения электромагнитного излучения конструкций экранов, выполненных на его основе / С. Э. Саванович, Т. В. Борботько // Весці Нац. акадэміі навук Беларусі. Серыя фізіка-тэхнічных навук. – 2021. – № 1. – С. 93–100.

9. Лушина, М. В. Современные экранирующие и радиопоглощающие материалы / М. В. Лушина, С. Г. Паршин, А. А. Ржевский // Системы управления и обработка информациию – 2011. – № 22. – С. 208–214.

10. Неамах, М. Р. Радиоэкранирующие модульные конструкции на основе порошкообразных материалов / М. Р. Неамах [и др.] ; под ред. Л. М. Лынькова. – Минск : Бестпринт, 2013. – 210 с.

УДК: 621.391:621.396

АНАЛИЗ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ ПРИ ВОЗДЕЙСТВИИ МОЩНЫХ ЭЛЕКТРОМАГНИТНЫХ ИМПУЛЬСОВ

Н.В. НАСОНОВА, Г.А. ПУХИР
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Введение. За последнее десятилетие наблюдается быстрый рост информационных систем всех видов, снижение уровней полезных сигналов при одновременном повышении количества и мощности различного электрооборудования, способного создавать высокий уровень помех. Подобные сбои могут привести к крупным экологическим катастрофам и большим человеческим жертвам [1]. Невыполнение требований электромагнитной совместимости способно причинить значительный материальный ущерб из-за сбоев систем управления автоматических производственных линий, неустойчивой работы линий связи, потери информации в компьютерах и т. д.

Для достижения принципиально нового уровня радаров, радиосвязи, технологий и других технических задач в ряде стран разрабатываются генераторы мощных электромагнитных импульсов. Генераторы мощных импульсов от одной до десятков наносекунд (линейные индукционные ускорители электронов, релятивистские генераторы с виртуальным катодом (виркаторы), релятивистские магнетроны, генераторы на основе сверхразмерных электродинамических структур (черенковские генераторы) и генераторы дифракционного излучения) интенсивно развиваются. Эти генераторы имеют пиковую мощность в гигаватт, и есть реальные способы ее увеличения в десятки раз. Достигнутые и прогнозируемые параметры излучения этих устройств делают их опасными при воздействии на радиоэлектронные системы самого широкого назначения [2]. Это связано с тем, что их режим работы позволяет генерировать и излучать в окружающее пространство не только одиночные электромагнитные импульсы, но и их «пакеты» с частотой тысяч импульсов в секунду и более.

1. Анализ природы источников мощного электромагнитного излучения. На сегодняшний день можно выделить несколько типов средств преднамеренного воздействия мощным электромагнитным излучением (ЭМИ) [3]:

1. *Электромагнитные средства летального действия* (основным поражающим фактором которого является электромагнитное излучение в диапазоне 100МГц…300 ГГц (максимум спектральной плотности или средняя частота излучения) с энергией в импульсе не менее 100 Дж (или пиковая мощность более 100 МВт или средняя мощность свыше 1 МВт).
2. *Средства генерации большой мощности для силовых систем РЭБ.* Предполагается использование метода генерации наносекундных мощных импульсов для их практического использования при создании перспективных систем силовой радиоэлектронной борьбы поражения радиоэлектронных систем (РЭС).
3. *Электромагнитные средства нелетального действия* (оружие, воздействующее на личный состав противника энергией электромагнитного излучения для кратковременного (от секунд до нескольких часов) лишения его боеспособности (создания условий для невозможности выполнять поставленные задачи).
4. *Средства направленного электромагнитного воздействия на окружающую среду* (объединяются некоторые разновидности метеорологического и геофизического оружия, использующих в качестве основного воздействующего фактора энергию ЭМИ).

Установки сверхкоротких импульсов состоят из генераторов импульсов с малой длительности и излучающих антенн, позволяют создавать направленное излучение со следующими параметрами: длительность импульсов от 0,1 до 0,3 нс; длительность фронта импульса от 85 до 250 пс; амплитуда напряженности электрического поля 56 кВ/м на расстоянии 100 м; частоты повторения импульсов варьируются от сотен герц до нескольких килогерц.

Конкретно элементами подсистем, на которые осуществляется электромагнитное воздействие или от которых необходимо анализировать ЭМИ, являются [4]: функциональные узлы цифровых электронных средств на основе печатных плат, цифровые электронные средства, кабельные (неэкранированная витая пара, коаксиальный кабель) системы, металлоконструкции; системы электропитания.

Наиболее чувствительной к воздействию сверхкоротких электромагнитных импульсов (СК ЭМИ) являются телекоммуникационные системы. При воздействии сверхкороткоимпульсных импульсно-периодических ЭМИ наибольшую опасность для радиоэлектронных систем являются импульсные помехи, наводимые в «паразитных» антеннах. На практике, воздействие СК ЭМИ на телекоммуникационные системы приводит к потере (искажению) информации, ложным срабатываниям систем охранной, пожарной и др. сигнализаций, сбоям в работе оборудования, блокирование каналов передачи информации (как проводных, так и беспроводных), сбоям и отказам электронных устройств [5].

Исследования [6] показали, что в общем случае воздействующими факторами на элементы телекоммуникационных систем (ТКС) при воздействии ЭМИ являются:

1) электромагнитные поля, проникающие через экраны конструкций элементов ЛВС и соединительные разъемы;

2) импульсные напряжения и токи в печатных платах элементов ТКС, наводимые электромагнитными полями, проникающими через неоднородности корпусов серверов и маршрутизаторов;

3) импульсные напряжения и токи, наводимые в цепях «экран-жила» соединительных кабелей и проводов, таких как витая пара.

Даже такие известные помехоустойчивые технологии, как оптоволоконные, оказываются подверженными воздействию мощных электромагнитных импульсов за счет воздействия на микроэлектронные компоненты, осуществляющие опто-электронные преобразования, а также из-за изменения вектора поляризации света в оптическом волокне под действием импульсных магнитных полей, которые могут возникать вокруг электрических проводах при наведении в них больших импульсных токов [7].

Воздействие мощного электромагнитного излучения на высокочувствительное электронное оборудование приводит к изменению параметров или полному выходу из строя устройств, что связано с переходом приемного и усилительного трактов в несогласованный режим и возникновением перенапряжений в элементной базе. В этом случае значение амплитуды или мощности воздействующего электромагнитного излучения может быть намного меньше пороговых значений, определяющих возникновение эффектов деградации в отдельных элементах и узлах. Значимость этих эффектов возрастает с увеличением функциональной сложности радиоэлектронной аппаратуры. Для обеспечения надежной работы радиоэлектронных средств в условиях внешних воздействий, в том числе мощного импульсного электромагнитного излучения, необходимо использование соответствующих средств защиты. Разработанные к настоящему времени методы и средства защиты радиоэлектронных средств не могут обеспечить требуемую эффективность их защиты по своим характеристикам, а тем более с учетом перспектив разработка средств генерации мощных импульсных электромагнитных излучений. Это обстоятельство требует исследований, направленных в первую очередь на поиск принципиально новых подходов к эффективной защите радиоэлектронных средств от мощного импульсного электромагнитного излучения, что ставит задачу исследования способов и механизмов воздействия мощных электромагнитных излучений на радиоэлектронные средства.

2. Перспективные методы защиты от воздействия источников мощного электромагнитного излучения. Под явлениями большой энергии приняты электрические поля с напряженностью свыше 100 В/м. Выбор частотного диапазона связан с тем, что достаточно интенсивные сигналы в диапазоне от 200 МГц до 5 ГГц вызывают повреждения во многих системах, а также с возможностями современных излучателей. Стандарты МЭК 61000-2-13 и ГОСТ 52863-2007 [8, 9] предусматривают требования и испытания технических средств на

устойчивость к воздействию СК ЭМИ длительностью от 0,1 до 0,8 мс при напряженности импульсного электрического поля от 0,02 кВ/м (для импульсов с высокой частотой повторения) до 30 кВ/м (для импульсов с низкой частотой повторения) в зависимости от степени жесткости этих испытаний. Накопленный опыт исследований и испытаний элементов объектов информатизации на устойчивость к преднамеренному силовому электромагнитному воздействию (ПД ЭМВ) показывает, что для обеспечения устойчивой работы автоматизированной системы в защищенном исполнении (АСЗИ) необходимо принятие специальных организационно-технических мер. Требования к организации и содержанию работ по защите АСЗИ от ПД ЭМВ, к средствам защиты АСЗИ от ПД ЭМВ и к средствам их обнаружения устанавливаются соответствующими стандартами.

Комплексный подход в защите информации актуален и в данном направлении. Он предусматривает весь возможный спектр мероприятий от использования более надежных микросхем, выдерживающих большее напряжение и токи, предохранителей и ограничительных устройств, до резервного копирования программных продуктов и информационных активов, позволяющего ускорить восстановление после сбоев. К дополнительным техническим мерам можно отнести фильтрацию опасных сигналов и экранирование ЭМИ.

Все методы защиты можно разделить на группы: конструкционные, схемотехнические и структурно-функциональные. Основным конструкционным методом защиты радиоэлектронной аппаратуры от воздействия внешних электромагнитных полей является экранирование. Защита портов электропитания, связи и управления от электрического пробоя и последующего температурного разрушения вследствие индуктированного влияния импульсного электромагнитного поля большой напряженности на проводные линии возлагается на ограничители от перенапряжений [10]. Такими элементами являются разрядники, выравниватели, варисторы, стабилитроны, быстродействующие защитные TVS диоды.

Мощность излучения, воздействующего на внутренние цепи радиоэлектронных средств P_{imp}, связана с потоком падающей мощности $\Pi(r)$ следующим соотношением

$$\mathrm{P_{imp}} = \Pi_{(\mathrm{r})} \cdot \mathrm{S_{eff}}(\mathrm{f}), \tag{1}$$

где $\Pi_{(r)}$ – вектор Умова-Пойнтинга;

$S_{eff}(f)$ – эффективная поверхность объекта.

Целесообразно оценивать защитные свойства экранирующих материалов по эффективности экранирования с учетом частотного диапазона электромагнитного импульса как отношение амплитуды напряженности импульсного электрического поля E_{P1} измеренной без образца защитного экрана и амплитуды E_{P2}, измеренной при наличии образца защитного материала экрана:

$$S_{EP} = 20\lg\left(\frac{E_{P1}}{E_{P2}}\right), \text{ dB}. \tag{2}$$

Широко известны радиопоглощающие структуры, представляющие собой вспененные материалы с полимерными металлизированными пленками, иглопробивные и войлочные материалы с проводящими наполнителями (например, содержащие углеродные нити или волокна), материалы с ферромагнитными включениями, тканые материалы, пропитанные растворами электролитов, такими как вода, водные растворы NaCl и $CaCl_2$ [11], [12], [13].

Эффективность экранирования СК ЭМИ иглопробивными материалами с добавками углерода (сухой материал) при воздействии ЭМИ с длительностью фронта излучаемого электромагнитного импульса/длительностью импульса 139/242 пс составляет 2…12,2 дБ (в зависимости от количества слоев), эффективность экранирования составляет 10,1…15,5 дБ для этого материала, пропитанного обычной водой, а эффективность экранирования составляет 12,0…15,5 дБ для материала, пропитанного насыщенным водным раствором NaCl. Результаты представлены для частотного диапазона 0,17–2,31 ГГц при мощности воздействующего импульсного излучения 5,34 МВт.

Эффективность экранирования для предложенного сверхширокополосного поглотителя ЭМИ составляет 11,9…13,9 дБ для войлочной ткани со слоем металлизированной полимерной пленки, пропитанной водным раствором $CaCl_2$, и 9,4… 12,1 дБ для вспененного полиэтилена с металлизированной пленкой.

Заключение. К числу наиболее опасных для защищаемых объектов видов мощных электромагнитных воздействий СК ЭМИ, длительность которых имеет порядок 150...1000 пс. Они характеризуются весьма высокой эффективностью воздействия на информационные, вычислительные и телекоммуникационные системы различного назначения. Несмотря на высокие амплитуду (обычно 1…100 кВ/м) и мгновенную мощность, для генерации СК ЭМИ требуется затратить сравнительно небольшую энергию, поэтому устройства их генерации получаются компактными и легкими. Сочетание этих факторов дает основание относить СК ЭМИ к одному из самых опасных видов поражающих воздействий. Таким образом, многочисленные экспериментальные и теоретические исследования свидетельствуют об опасности возможного использования СК ЭМИ для вывода из строя радиоэлектроники систем и объектов различного назначения, включая вооружения и военную технику, а также высокую вероятность использования СК ЭМИ как средства электронного терроризма и гибридных военных действий.

Эффективный способ, который позволяет обеспечить требования электромагнитной экологии, снизить до приемлемого уровня естественные и искусственные помехи при работе радиоэлектронных систем, основан на применении экранирующих и радиопоглощающих материалов (РПМ) и покрытий (РПП). Последние являются также перспективным средством снижения радиолокационной заметности (РЛЗ) объектов военной техники (самолетов, кораблей, ракет, наземного стационарного и мобильного оборудования и. т. д.). Использование РПМ и РПП существенно расширяет возможности технологий Stealth, с помощью которых создаются объекты с низким уровнем РЛЗ. РПП могут быть использованы и для защиты компьютерных систем обработки информации от несанкционированного доступа, в космической техники, для поглощения электромагнитного излучения в экранирующих устройствах, в поглощающих облицовках и корпусах, а также в безэховых измерительных камерах.

В настоящее время в качестве РПМ используются ферритовые материалы, материалы на основе тонких пленок углерода с ферромагнитными наночастицами, нанесенными на гибкую подложку [12] или инкорпорированных в полимерное связующее, а также различные волокнистые основы, жидкими растворными наполнителями. Эффективность экранирования мощных электромагнитных импульсов такими РПМ в сверхшироком диапазоне частот 0,17…300 ГГц может достигать 10…60 дБ, а коэффициентом отражения до –10…–20 дБ при снижении приведенной удельной массе (на единицу площади) до 1–1,5 кг/м^2. Конструктивные преимущества иглопробивных и войлочных материалов, малый удельный вес и цена позволяют рассматривать эти материалы как перспективные с точки зрения защиты электронной аппаратуры от внешних воздействий электромагнитного излучения (в том числе СК ЭМИ).

Список литературы

1. Чаплыгин, А. В. Электромагнитная совместимость электронных технических средств. Реальная необходимость или необходимая реальность / А.В. Чаплыгин, А.В. Гребенкин // Алгоритм безопасности. – 2017. – № 5. – С. 54–57.

2. Кечиев, Л. Н. ЭМС и информационная безопасность в системах телекоммуникаций / Л. Н. Кечиев, П. В. Степанов. – М. : Издательский Дом «Технологии», 2005.

3. Быстров, Р. П. Электромагнитные системы и средства преднамеренного воздействия на физические и биологические объекты / Р. П. Быстров // РЭНСИТ. – 2014. – Т. 6 (2). – С. 129–169.

4. Агапов, С. В. Защита информации в цифровых электронных средствах интеллектуальных зданий при электромагнитных воздействиях / С. В. Агапов, З. М. Гизатуллин, С. Ф. Чермошенцев // Технологии ЭМС. – 2010. – № 3 (34). – С. 3–21.

5. Акбашев, Б. Б. Механизм деструктивного воздействия мощных сверхширокополосных импульсов на радиоэлектронные системы / Б. Б. Акбашев, Д. И. Еряшев, А. Н. Корнев // Технологии ЭМС. – 2011. – № 2 (37). – С. 21–25.

6. Экспериментальные исследования функционирования устройств типовой комплексной системы безопасности в условиях воздействия сверхкоротких электромагнитных полей / Б. Б. Акбашев [и др.] // Технологии ЭМС. – 2011. – № 2 (37). – С. 32–38.

7. Проблема электромагнитных воздействий на микропроцессорные устройства релейной защиты. Часть 3. Гуревич В. // Компоненты и технологии. – 2010. – № 4. – С. 91–96.

8. МЭК 61000-2-13. Electromagnetic compatibility (EMC). – Part 2–3: Environment – High-power electromagnetic (HPEM) environments – radiated and conducted», 2004. − P. 16.

9. ГОСТ Р 52863-2007 Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие положения. – М. : Стандартинформ, 2008. – 34 с.

10. Довбыш, В. Н. Электромагнитная безопасность элементов энергетических систем / В. Н. Довбыш, М. Ю. Маслов, Ю. М. Сподобаев. – Самара : ООО «ИПК «Содружество», 2009. – 198 с.

11. Экранирующие характеристики текстильных растворосодержащих матриц / Н.В.Ковальчук [и др.] // Доклады БГУИР. – 2011. – № 8 (62). – С. 27–33.

12. Экраны электромагнитного излучения на основе магнитных материалов. Технологии. Конструкции. Применение / А.А. Ахмед [и др]; под ред. Л.М. Лынькова – Минск : Бестпринт, 2016. – 223 с.

13. Николайчук, Г. Радиопоглощающие материалы на основе наноструктур / Г. Николайчук, В. Иванов, С. Яковлев // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. – 2010. – № 1. – С. 92–95.

УДК 537.86; 004.056.5

О НЕКОТОРЫХ СВОЙСТВАХ ФУНКЦИЙ ИДЕНТИФИКАЦИИ НЕЛИНЕЙНЫХ ОБЪЕКТОВ

А.Г. ФИЛИППОВИЧ
Оперативно-аналитический центр при Президенте Республики Беларусь, г. Минск, Республика Беларусь

Аппаратура нелинейной радиолокации является достаточно эффективным инструментом поиска и обнаружения специальных технических средств негласного получения информации (далее – закладные устройства). С помощью нелинейного радиолокатора можно обнаруживать признаки присутствия закладных устройств, установленных в укрывающих средах, по наличию отклика от входящих в его конструкцию нелинейных элементов.

Основной проблемой, с которой сталкиваются специалисты, является идентификация обнаруженного нелинейного объекта. В рамках процедуры идентификации закладного устройства необходимо последовательно решить две задачи:

- является ли обнаруженный нелинейный объект, установленный в укрывающих средах, объектом естественного происхождения (например, ржавая арматура в бетонной стене) или это искусственно созданный объект;
- если обнаруженный нелинейный объект является искусственно созданным, может ли он быть классифицирован как составной элемент закладного устройства.

Использование классических средств нелинейной радиолокации для целей идентификации закладных устройств ограничено и не всегда эффективно [1]. В качестве альтернативы в работе [1] предложен новый подход, основанный на оценке функции идентификации закладных устройств методом нелинейного радиочастотного сканирования. В рамках данной работы сделана попытка оценки потенциальной эффективности предложенного подхода.

Для решения указанной задачи необходимо рассмотреть свойства функций идентификаций нелинейных объектов, предложенных в [1]. Можно показать, что данные функции для второй и третьей гармоник зондирующего сигнала нелинейного радиолокатора могут быть представлены в виде:

$$\hat{J}_2(\omega, P_{\text{изл}}) = \frac{U_{2np}}{U_{э2np}} \sqrt{\xi 2_э(\omega, P_{\text{изл}})},$$
$$\hat{J}_3(\omega, P_{\text{изл}}) = \frac{U_{3np}}{U_{э3np}} \sqrt{\xi 3_э(\omega, P_{\text{изл}})}, \quad (1)$$

где $\xi 2_э(\omega, P_{\text{изл}})$, $\xi 23(\omega, \text{Ризл})$ – функции нелинейного преобразования эталонного нелинейного объекта на частоте второй и третьей гармоник зондирующего сигнала:

U_{2np}, U_{3np} – функции напряжения на входе приемного тракта нелинейного радиолокатора на частоте второй и третьей гармоник зондирующего сигнала, переизлученного обнаруженным нелинейным объектом;

$U_{э2np}$, $U_{э3np}$ – функции напряжения на входе приемного тракта нелинейного радиолокатора на частоте второй и третьей гармоник зондирующего сигнала, переизлученного эталонным нелинейным объектом;

$P_{\text{изл}}$ – мощность излучения нелинейного локатора;

ω – круговая частота.

В качестве эталонного нелинейного объекта выберем полупроводниковый диод. Физически такой объект представляет собой *p-n* переход, нагруженный на вибраторную антенну [2]. Эквивалентная схема эталонного нелинейного объекта представлена на рисунке 1.

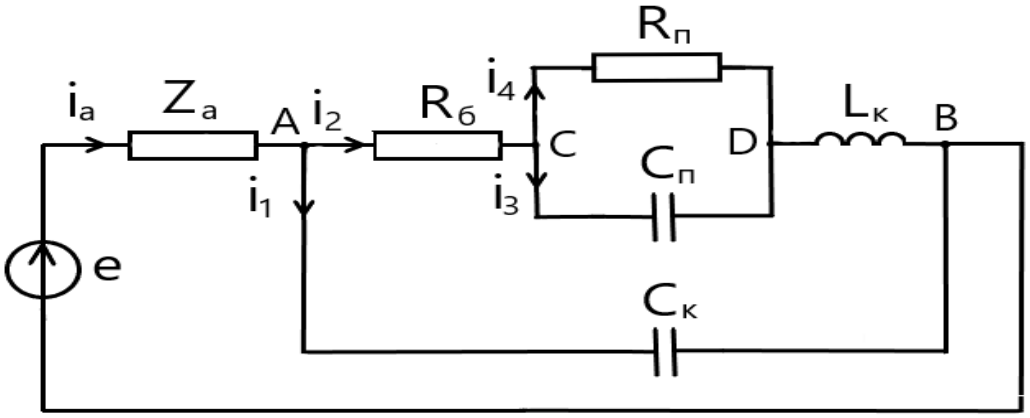


Рис. 1. Эквивалентная схема эталонного нелинейного объекта: Z_A – комплексное сопротивление антенны, к которой подключен p-n переход; $R_б$ – сопротивление базы; $C_к$ – контактная емкость; $L_к$ – индуктивность контакта; R_n – активное сопротивление p-n перехода; C_n – емкость p-n перехода; e – э. д. с., создаваемая в антенне нелинейного объекта зондирующим сигналом нелинейного локатора

В соответствии с уравнением (1) функции идентификации эталонного нелинейного объекта совпадают с функциями нелинейного преобразования. Получим выражения для этих функций с учетом ряда начальных условий.

Во-первых, предположим, что зондирующий сигнал нелинейного радиолокатора является монохроматическим. В этом случае э. д. с., возникающая в нелинейном объекте, может быть представлена в виде:

$$e(t)=U_m\cos(\omega_0 t)\ , \tag{2}$$

где U_m – амплитуда э.д.с., возникающей в нелинейном объекте;

ω_0 – круговая частота зондирующего сигнала нелинейного радиолокатора.

Во-вторых, поскольку выражения (1) имеют функциональную зависимость от частоты, необходимо определить диапазон частот, в пределах которого будет проводиться анализ. Исходя из экспериментальных данных, представленных, например, в работе [3], границы частотного диапазона зондирующего сигнала нелинейного локатора целесообразно ограничить диапазоном 0,3..4ГГц. В этом случае диапазон частот сигнала второй гармоники будет составлять 0,6..8ГГц, третьей – 0,9..12 ГГц.

В-третьих, поскольку в качестве эталонного нелинейного объекта был выбран полупроводниковый диод. Антенна такого эталонного нелинейного объекта представляет собой короткий вибратор. Определим, что длина плеча такого вибратора l=0,005 м, а толщина a_0 = 0,0005 м, что приблизительно соответствует физическим размерам контактных «ножек» реального полупроводникового диода. В этом случае комплексное сопротивление антенны нелинейного объекта может быть представлено в виде [4]:

$$z_a = R_a + jX_a = 80\pi^2\left(\frac{1}{\lambda}\right)^2 - j120\left(\ln\left(\frac{2l}{a_0}\right)-1\right)ctg\left(\frac{2\pi l}{\lambda}\right), \tag{3}$$

где R_a – действительная часть комплексного сопротивления антенны нелинейного объекта;

X_a – мнимая часть комплексного сопротивления антенны нелинейного объекта;

λ – длина волны.

В-четвертых, ограничимся рассмотрением случая, когда к диоду приложено прямое напряжение, поскольку в режиме обратного включения существует слабая зависимость величины тока, протекающего через диод, от приложенного к нему напряжения. Данное обстоятельство накладывает ограничение на вариативность функций идентификации. Кроме того, ввиду небольшой амплитуды обратного тока, возникающего в импедансе антенны эталонного нелинейного объекта, переизлученный сигнал нелинейного радиолокатора будет трудно различим на фоне внешнего электромагнитного фона.

С учетом принятых допущений можно показать, что выражения для функций идентификации могут быть представлены в следующем виде:

$$\lambda_{2э}\left(\omega,\mathrm{P}_{изл}\right)=\frac{1}{4}i_s U_m\left(\frac{q}{kT}\right)^2\left(\frac{R_n}{|\sigma|}\right)|Z_a|\sqrt{1+|A|^2+2|A|\cos(A)}e^{j(Z_a-B_2)};$$
$$\lambda_{3э}\left(\omega,\mathrm{P}_{изл}\right)=\frac{1}{24}i_s U_{m^2}\left(\frac{q}{kT}\right)^3\left(\frac{R_n}{|\sigma|}\right)|Z_a|\sqrt{1+|A|^2+2|A|\cos(A)}e^{j(Z_a-B_3)}, \quad (4)$$

где $q \approx 1{,}6\times10^{-19}$ Кл – заряд электрона;

$k \approx 1{,}38\times10^{-23}$ Дж·Кл$^{-1}$ – постоянная Больцмана;

T – абсолютная температура;

i_s – ток насыщения диода.

$$|Z_a|=\sqrt{\left[80\pi^2\left(\frac{1}{\lambda}\right)^2\right]^2+\left[120\left(\ln\left(\frac{2l}{a_0}\right)-1\right)\mathrm{ctg}\left(\frac{2\pi l}{\lambda}\right)\right]};$$

$$Z_a=\mathrm{arctg}\left(\frac{120\left(\ln\left(\frac{2l}{a_0}\right)-1\right)\mathrm{ctg}\left(\frac{2\pi l}{\lambda}\right)}{80\pi^2\left(\frac{1}{\lambda}\right)^2}\right);$$

$$|A|=\frac{i_2\omega C_к}{1+\omega^2 C_{п^2}R_{п^2}}\sqrt{\omega^2\left(C_п R_{п^2}-L_к-\omega^2 L_к C_{п^2}R_{п^2}\right)^2+\left(R_п+R_б+\omega^2 C_{п^2}R_{п^2}R_б\right)^2};$$

$$A=-arctg\left(\frac{R_п+R_б+\omega^2 C_{п^2}R_{п^2}R_б}{\omega\left(C_п R_{п^2}-L_к-\omega^2 L_к C_{п^2}R_{п^2}\right)}\right);$$

$$B_2=\mathrm{arctg}\left(\frac{\sin(2\sigma)+|A|\sin(2\sigma+\mathrm{A})}{\cos(2\sigma)+|A|\cos(2\sigma+\mathrm{A})}\right);$$

$$B_3=\mathrm{arctg}\left(\frac{\sin(3\sigma)+|A|\sin(3\sigma+\mathrm{A})}{\cos(3\sigma)+|A|\cos(3\sigma+\mathrm{A})}\right);$$

$$|\sigma|=\sqrt{\left(\left(1-\omega X_a C_к\right)R_п+m^2\right)+\left(\omega C_к R_a R_п+n\right)^2};$$

$$\sigma=\mathrm{arctg}\left(\frac{\omega C_к R_a R_п+n}{\left(1-\omega X_a C_к\right)R_п+m}\right);$$

$$m=R_a+R_б-\omega X_a\left(C_к R_б+C_п R_п\right)-\omega^2\left(C_к L_к R_а+C_к R_а C_п R_п R_б+C_п R_п L_к\right)+\omega^3 C_к X_a C_п R_п L_к;$$

$$n=X_a+\omega\left(C_к R_а R_б+L_к+C_п R_п R_б+C_п R_п R_а\right)-\omega^2 C_к X_a\left(L_к+C_п R_п R_б\right)-\ \omega^3 C_к R_a C_п R_п L_к;$$

$$C_п R_п=\frac{\tau}{1+\sqrt{1+\omega^2\tau^2}},$$

где τ – время жизни неравновесных носителей заряда.

Сопротивление p-n перехода зависит от амплитуды э.д.с., создаваемой нелинейным локатором в эталонном нелинейном объекте, и может быть получено численно из следующего уравнения:

$$\exp\left(\frac{q}{kT}\frac{U_m R_n}{2|\sigma|}\delta\left(\omega-\omega_0\right)\right)=\frac{kT\sqrt{2}}{i_s q a R_n}, \quad (5)$$

где $a=\sqrt{1+\sqrt{1+\omega^2\tau^2}}$.

Таблица 1

Параметр	Д311	КД522
$L_к$, мкГн	0,01	0,01
$C_к$, пФ	1,5	2,2
$R_б$, Ом	40	40
i_s, мкА	100	2
τ, с	10^{-7}	10^{-7}

Для анализа функций идентификации (4) в качестве эталонных нелинейных объектов выберем германиевый диод Д311 и кремниевый диод КД522, характеристики которых представлены в таблице 1. Как видно из таблицы, основным отличием физических характеристик диодов является различие в величине обратного тока. У кремниевых диодов она существенно ниже, что является следствием большего значения ширины запрещенной зоны. Данное свойство также влияет на величину крутизны нижнего загиба прямой ветви вольтамперной характеристики, что в свою очередь будет влиять на величину сопротивления *p-n* перехода в соответствии с уравнением (5).

Графики функций идентификации (4) для диодов Д311 и КД522 в диапазоне частот зондирующего сигнала 300...4000 МГц представлены на рисунках 2 и 3. Вид функций идентификации диодов Д311 и КД522, представленных на графиках рисунков 2 и 3, объясняется резонансными явлениями в электрической цепи эталонного нелинейного объекта в рассматриваемом диапазоне частот.

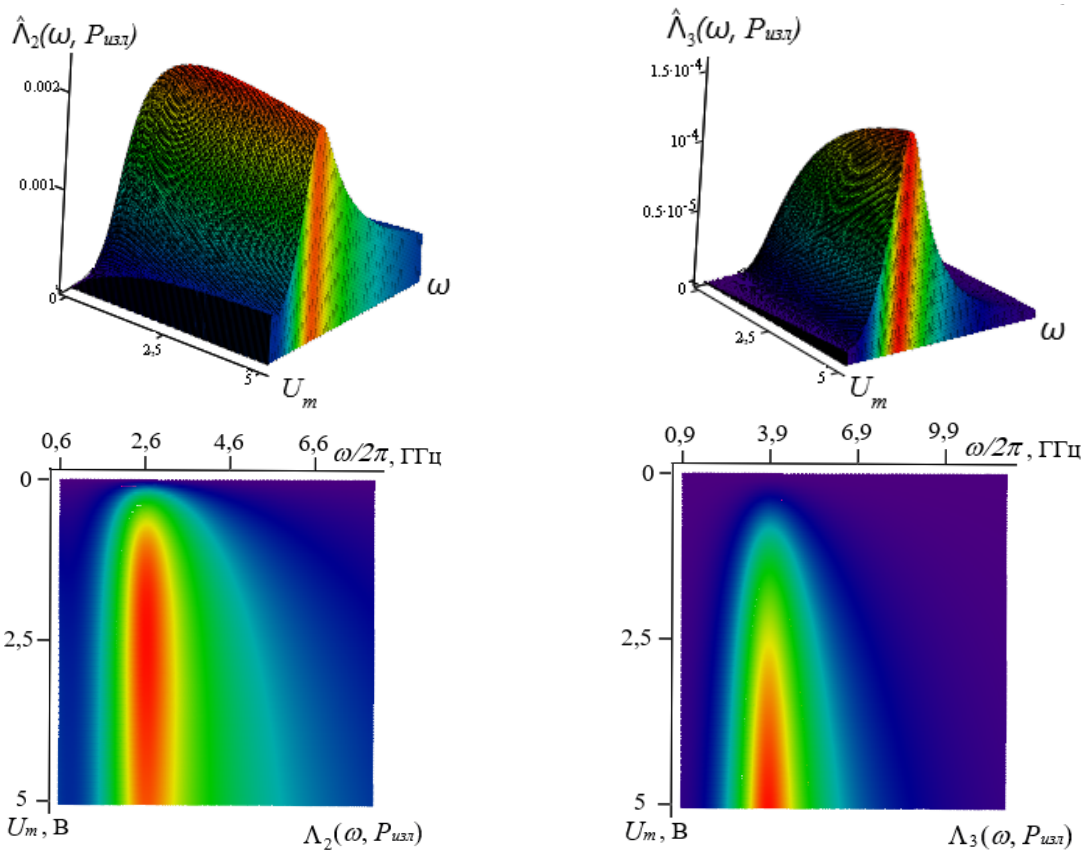


Рис. 2. Графики функций идентификации диода Д311

Вид функциональных зависимостей (4) может быть объяснен с позиции теории, изложенной в работе [5]. Экстремумы функций идентификации могут смещаться по оси частот при изменении значений параметров эквивалентной схемы диода. Область значений функции идентификации для второй гармоники на порядок больше, чем для третьей. Это объясняется особенностями функциональной зависимости вольт-амперной характеристики p-n перехода.

В диодах Д311 и КД522 значения индуктивностей и емкостей элементов, входящих в эквивалентную схему, отличаются незначительно. Поэтому максимумы функций идентификации сосредоточены приблизительно в одном диапазоне частот зондирующего сигнала нелинейного локатора (в области частоты 1300 МГц). Однако вариативность функции (4) при изменении частоты для диода КД522 ниже, чем для диода Д311, что может быть объяснено более высоким сопротивлением p-n перехода при одинаковом входном напряжении (меньшим значением тока насыщения).

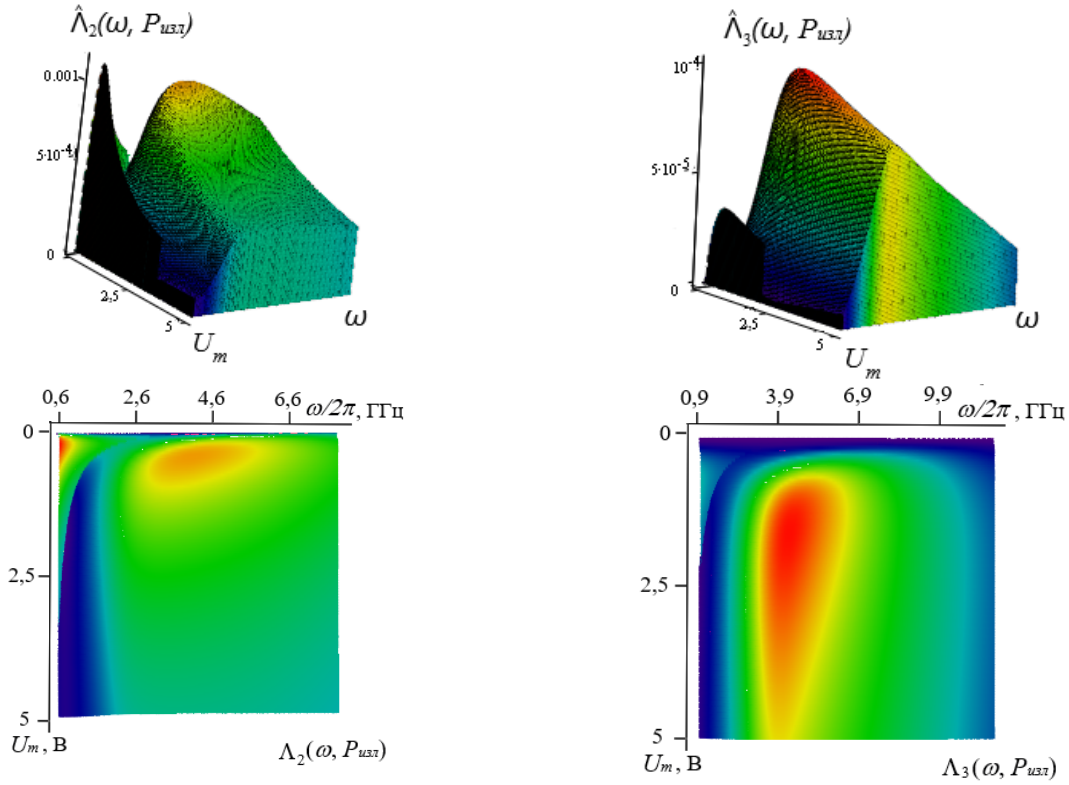


Рис. 3. Графики функций идентификации диода КД522

Более детальный анализ свойств функций (4) позволяет сделать вывод о возможности их эффективного применения для идентификации нелинейных объектов, выполненных из разных материалов и обладающих разными физическими свойствами.

Список литературы

1. Филиппович, А. Г. О некоторых вопросах идентификации объектов в нелинейной радиолокации / А. Г. Филиппович // Комплексная защита информации : тез.и докл. Междунар. науч.-практ. конф., Москва, 15-17 сентября 2020 г. – С. : Медиа Группа «Авангард», 2020. – С. 220–223.

2. Щербаков, Г. Н. Исследование рассеивающих свойств нелинейного биконического отражателя – физической модели боеприпаса с электронными устройствами / Г. Н. Щербаков [и др.] // Специальная техника и связь. – 2011. – № 1. – С. 33–39.

3. Бельчиков, А. В. Взгляд разработчиков нелинейных локаторов серии «Лорнет» на некоторые актуальные вопросы нелинейной локации / А. В. Бельчиков [и др.] // Специальная техника. – 2011. – № 5. – С. 40–46.

4. Неганов, В. А. Современная теория и практические применения антенн / В. А. Неганов, Д. П. Табаков, Г. П. Яровой. – М. : Радиотехника, 2009 – 720 с.

5. Штейншлейгер, В. Б. Нелинейное рассеяние радиоволн металлическими объектами / В. Б. Штейншлейгер // Успехи физических наук. – 1984. – Т. 142, вып. 1. – С. 131–145.

УДК 681.327.8.

ОЦЕНКА ЗАЩИЩЕННОСТИ НИЗКОЧАСТОТНЫХ КАНАЛОВ УТЕЧКИ, ОБРАЗОВАННЫХ ЭЛЕКТРИЧЕСКИМИ И МАГНИТНЫМИ ИНФОРМАЦИОННЫМИ ПОЛЯМИ РАССЕИВАНИЯ

В.К. ЖЕЛЕЗНЯК, М.В. ИЗОИТКО
Полоцкий государственный университет, г. Новополоцк, Республика Беларусь

Введение. Низкочастотные (НЧ) поля являются источниками утечки информации, которые обусловлены побочными излучениями речевых сигналов электрических и магнитных полей рассеивания. Таким образом, целью работы является оценка и калибровка электрических и магнитных полей рассеивания от утечки информации.

Для исследования электрических и магнитных полей рассеивания необходимы высокочувствительные первичные измерительные преобразователи с известными основными измерительными параметрами: размерностями их единиц [1], а также источники электрических и магнитных полей [1, 2]. При анализе электромагнитных полей важное значение имеют понятия о ближней и дальней зонах распространения электромагнитной энергии в зависимости от расстояния до источника измерения в предположении, что размеры излучателя l □ λ, где λ – длина волны излучения. В ближней зоне на относительных расстояниях от источника $r \le \lambda/2\pi \le 1$ поле еще не сформировалось в плоскую волну и может представлять собой (рис. 1) преимущественно поле магнитной индукции H, если в источнике протекает значительный ток, при относительно малом напряжении, или поле электрической индукции E, если в источнике протекает малый ток при относительно большом напряжении. Понятие «преимущество» означает, что ближняя зона всегда характеризуется двумя составляющими индукции H и E, но в зависимости от характеристик источника, может преобладать одна из составляющих.

НЧ электрические и магнитные поля рассеивания в ближней зоне [3] для измерения и испытания первичных измерительных преобразователей необходимо сформировать источники электрических из [3] и магнитных полей в ближней зоне.

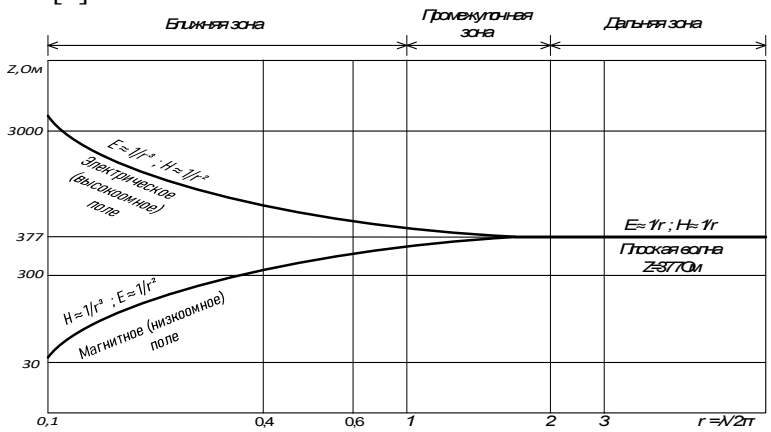


Рис. 1. Волновые сопротивления электрической (E) и магнитной (U) составляющих поля ближней зоны распространения в зависимости от расстояния до источника излучений

$$R = \lambda/2\pi.$$

Расчет электрического поля. Численные значения величин напряженности электрического поля определены на основании размерности единицы ее физической величины. Единицей физической величины напряженности поля является В/м. Вольт на метр напряженности однородного электрического поля, создаваемого разностью потенциалов 1 В между точками, находящимися на расстоянии поля [5]. Для расчета и измерения электрического поля используем конденсатор с параллельными пластинами [5] в отличие от расчета напряженно-

сти электрического поля, выполненного в работе [1] как более сложный. Емкость конденсатора с двумя параллельными пластинами определяется [5]:

$$C = \frac{S}{d}\ (м) = 3{,}33\,м,$$

где S – площадь двух пластин, (м^2);

d – расстояние между двумя пластинами, $d = 0.3м$.

При подаче от источника напряжения (генератор низкочастотных сигналов с симметричным выходом) 1 В получаем $\frac{B}{м} = \frac{1}{3.33}$. Вводим в геометрический центр конденсатор с двумя пластинами с размером 1 м × 1 м каждый первичный измерительный преобразователь, геометрический центр которого совпадает с геометрическим центром конденсатора.

Измеряем напряжение гармонического измерительного сигнала на выходе первичного измерительного преобразователя селективным вольтметром. Одновременно к пластинам приложено напряжение 1 В.

Емкость эталона поля определяется по формуле:

$$C_п = \frac{S^2}{d}\ (м), \tag{1}$$

где S – площадь двух пластин, м^2;

d – расстояние между двумя пластинами, м.

Напряженность поля внутри пластин при подаче на обкладки напряжения:

$$E_э = \frac{B_э}{M_э} = \frac{1B}{3{,}33м} = 0{,}3\frac{B}{м} \tag{2}$$

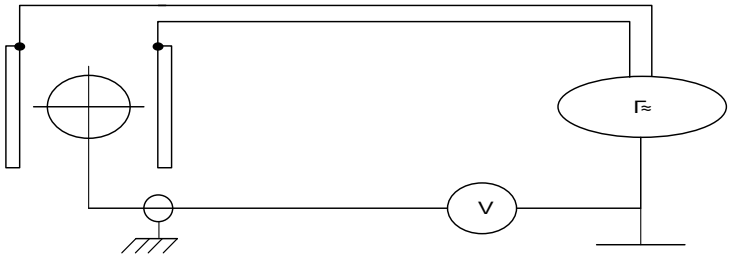


Рис. 2. Схема измерительного преобразователя

Проверка первичного измерительного преобразователя выполняется введением его внутрь пластин. Она должна находиться в геометрическом центре конденсатора.

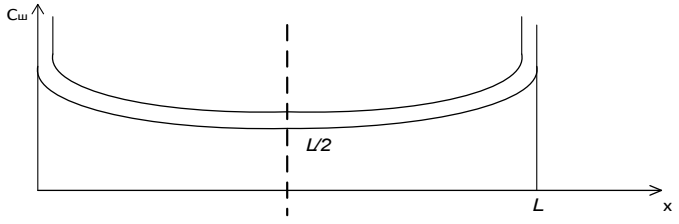


Рис. 3. Зависимость емкости измерительного преобразователя от координаты шара-зонда

На обкладки пластин подается эталонное напряжение с симметричного выхода генератора. Рассчитывается напряженность поля $E_э$. Измеряется напряжение поля с учетом коэффициента активного первичного измерительного преобразователя, который вычисляется следующим образом:

$$M_п = \frac{B_п \cdot M_э}{B_э}, \tag{3}$$

где $B_п$ – напряжение антенны; $M_э$ – коэффициент преобразования установки.

Расчет магнитного поля. Для создания переменного магнитного поля от 100 Гц до 10 кГц используются кольца Гельмгольца и кольца Максвелла [7]. Кольца Гельмгольца состоят из двух катушек и обладают большой неравномерностью магнитного поля. Кольца Максвелла состоят из пяти катушек, которые создают более равномерное магнитное поле.

В рабочем объеме пять колец Максвелла, на вход которых подается переменный ток I, создается слабое магнитное поле Н, А/м [1].

$$H = \frac{I \cdot K_в}{\mu_0} = \frac{B}{\mu_0}, \qquad 4)$$

где I – ток в кольцах, А;

$K_в$ – магнитная постоянная колец Максвелла;

μ_0 – магнитная проницаемость вакуума, равная $4\pi \cdot 10^{-7}$, $\left(\frac{B \cdot c}{A \cdot м}\right)$.

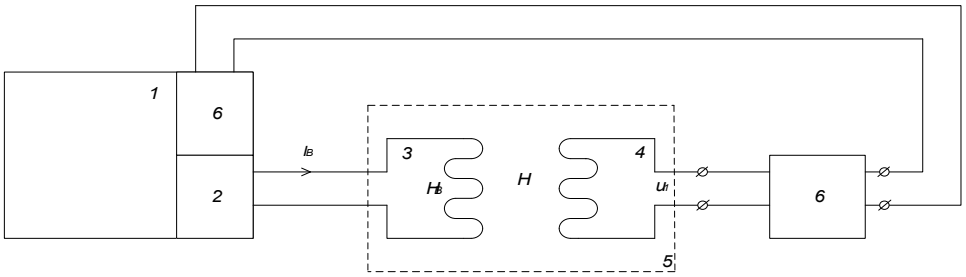


Рис. 4. Блок-схема калибровки магнитного измерительного преобразователя (ИП): *1* – измерительная система магнитного поля; *2* – НЧ генератор сигнала измерительной информации; *3* – кольца Максвелла; *4* – (ИП) магнитный; *5* – измерительное пространство колец Максвелла; *6* – селективный вольтметр

Коэффициент преобразования измерительного преобразователя магнитного поля $K_п$ определяется выражением:

$$K_п = \mu_0 2\pi f K_{sω} K_{ус}, \qquad (5)$$

где $K_{ус}$ – коэффициент усиления усилителя;

I – частота ИС;

$K_{sω}$ – постоянная измерительного преобразователя, м^2.

Значение $K_{sω}$ измерительного преобразователя определяется выражением:

$$K_{sω} = \frac{K_п}{\mu_0 2\pi f K_{ус}} \qquad (6)$$

Параметры ИП магнитного измеряются с помощью колец Максвелла в соответствии с блок-схемой, представленной на рис. 5.

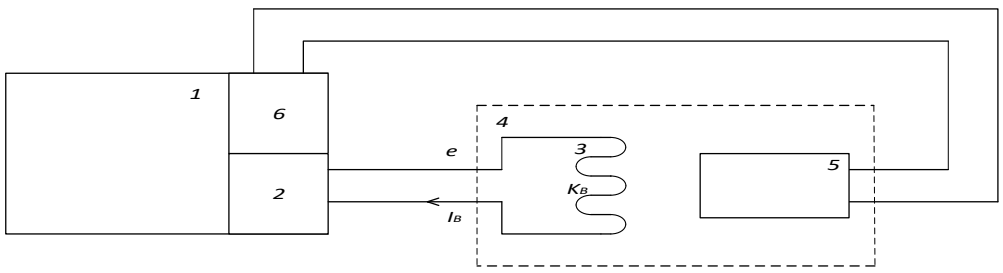


Рис. 5. Измерение магнитного момента исследуемого технического средства передачи (обработки): *1* – система измерительная автоматизированная; *2* – генератор сигналов измерительной информации низкочастотный; *3* – кольца Максвелла; *4* – измерительное пространство колец Максвелла; *5* – магнитная антенна; *6* – селективный вольтметр.

Ток $I_в$, протекая через кольца Максвелла, создает в замкнутом пространстве *5* напряженность поля.

$$H_м = \frac{I_в \cdot K_в}{\mu_0} \left(\frac{А}{м}\right),$$

где $K_в$ – магнитная постоянная для конкретной конструкции колец Максвелла.

Ток $I_в$, протекая через кольца Гельмгольца, создает в замкнутом пространстве *5* напряженность поля.

$$H_г = \frac{I \cdot S}{2\pi r^3} \left(\frac{А}{м}\right).$$

Для нормированного значения напряженности поля $H_т$ ток $I_в$ в кольцах Максвелла определяется из формулы:

$$I_в = \frac{\mu_0 \cdot H_Т}{K_в}.$$

Коэффициент преобразования $K_п$ ИП магнитного поля *4 с* усилителем *6* ($K_{ус}$ = 10) определяется выражением:

$$K_п = \mu_0 2\pi f K_{sω} K_{ус} \quad (7)$$

где $K_п$ – значение измерено в соответствии с блок-схемой;

$K_{ус}$ – коэффициент усиления усилителя *6*;

f – частота измерительного сигнала, 1 кГц;

$K_{sω}$ – постоянная ИП магнитного поля, м^2.

Из формулы (7) следует, что постоянная $K_{sω}$ ИП магнитного поля:

$$K_{sω} = \frac{K_п}{\mu_0 2\pi f K_{ус}}. \quad (8)$$

Использован измерительно-расчетный метод, основанный на измерении в точках, при которых значения напряженности поля превышает значения на границе контролируемой зоны (КЗ) с последующим пересчетом в точку КЗ.

Заключение. Показано, что каналы утечки электрического и магнитного полей рассеивания находятся в ближней зоне. Эти поля должны измерять обособленно, так как между ними отсутствует математическая зависимость.

Полученная установка измерения напряженности электрического поля с помощью конденсатора в виде параллельных плоских пластин и подачи на них эталонного напряжения обеспечивает калибровку (проверку) первичного измерительного преобразователя при внесении его в электрическое поле, измерением преобразованного на его выходе напряжения и определении коэффициента преобразования первичного измерительного преобразователя, что значительно упрощает и повышает чувствительность коэффициента преобразования.

Кольца Максвелла и Кольца Гельмгольца формируют эталонные напряженности поля, подачи на них эталонного тока обеспечивают калибровку первичных измерительных преобразователей магнитного поля при внесении их в область равномерного магнитного поля, что обеспечивает высокую помехозащищенность, высокую чувствительность коэффициента преобразования.

Список литературы

1. Железняк, В. К. Защита информации от утечки по техническим каналам : учеб. пособие / В. К. Железняк. – СПб., 2006. – 188 с.

2. Савельев, И. В. Курс физики : учебник : в 3-х т. Т. 2: Электричество. Колебания и волны. Волновая оптика. – М. : Наука, 1989. – 464 с.

3. Князев, А. Д. Конструирование радиоэлектронной и электронно-вычислительной аппаратуры с учетом электромагнитной совместимости / А. Д. Князев, А. Н. Кечиев, Б. В. Петров. – М. : Радио и связь, 1989. – 224 с.

4. Чертов, А. Г. Физические величины (терминология, определения, обозначения, размерности, единицы) : справ. пособие. – М. : Высш. шк., 1990. – 335 с.

5. Справочник по радиотехнике / под ред. Б. А. Смиренина. – М. : Гос. энерг. издательство, 1950. – 785 с.

6. ГОСТ Р 6746-94 «ГСИ. Меры электрической емкости. Общие технические требования»

7. Роткевич, В. Техника измерений при радиоприеме / В. Роткевич, П. Роткевич ; пер с польск. – М. : Связь, 1969. – 496 с.

УДК 621.391.82

ОЦЕНКА ЗАЩИЩЕННОСТИ КАНАЛОВ УТЕЧКИ ВИДЕОКАДРОВ ПАССИВНЫМИ МЕТОДАМИ ШИМ-ПРЕОБРАЗОВАТЕЛЯ

С.В. ХАРЧЕНКО, В.К. ЖЕЛЕЗНЯК
Учреждение образования «Полоцкий государственный университет», г. Новополоцк, Республика Беларусь

Цель доклада: провести анализ тонкой структуры информационных составляющих излучающихся сигналов ШИМ-преобразователя при питании СВТ и оценить эффективность внедрения схемно-конструктивных пассивных методов ЗИ при их внедрении в ШИМ-преобразователь при питании СВТ.

Для реализации цели необходимо выполнить следующие задачи:

1. Провести анализ тонкой структуры информационных составляющих излучающихся сигналов.

2. Предложить схемно-конструктивные пассивные методы ЗИ ШИМ-преобразователя СВТ. Внедрить предложенные схемно-конструктивные пассивные методы ЗИ.

3. На основе разработанной в докладе «Методика оценки защищенности видеоинформации ШИМ-преобразователя средств вычислительной техники (СВТ)» методики, провести анализ эффективности предложенных методов ЗИ.

Фильтрация. Необходимость использования фильтрации обуславливается тем, что информация может утекать по электрическим КУИ в виде кондуктивных помех, а фильтрация является основным средством ослабления кондуктивных помех.

Эффективность фильтрации определяется вносимым затуханием фильтра:

$$S = 20\lg\left|\frac{\dot{U}_1}{\dot{U}_2}\right|, \text{ или } S = 20\lg\left|\frac{\dot{I}_1}{\dot{I}_2}\right|, \quad (1)$$

где $\dot{U}_1, \dot{I}_1$ – напряжение и ток помех на нагрузке в исходном состоянии, $\dot{U}_2, \dot{I}_2$ – напряжение и ток помех на нагрузке в цепи с фильтром [2].

Основными требованиями, предъявляемыми к фильтру, являются следующие:

1. Обеспечение заданной эффективности фильтрации в требуемом частотном диапазоне $S(t)$;

2. Ограничение допустимого падения постоянного или переменного напряжения на фильтре при максимальном токе нагрузки;

3. Ограничения по требованиям техники безопасности допустимого значения реактивной составляющей тока на основной частоте;

4. Обеспечение допустимых нелинейных искажений питающего напряжения, определяющих требования к линейности фильтра;

5. Элементы фильтра должны выбираться с учетом номинальных токов и напряжений электрической цепи, а также возможных возникающих в ней бросков напряжений и токов, вызванных нестабильностью электрического режима и переходными процессами;

6. Конструктивные: эффективность экранирования, минимальные габаритные размеры и масса, обеспечение нормального теплового режима, стойкость к механическим и климатическим воздействиям, технологичность конструкции и т. д. [2]

Для ослабления широкополосной помехи на верхних частотах, в цепь прохождения сигнала следует включить те или иные разновидности фильтров нижних частот. Для ослабления узкополосной помехи используются узкополосные режекторные фильтры, а на частотах свыше 100 МГц, в качестве режекторных фильтров, часто используют полуволновые или четвертьволновые отрезки длинных линий.

Поскольку индуктивные фильтры отражают высокочастотные сигналы, они могут быть причиной стоячих волн и, следовательно, повышения уровня излучаемых помех. Кроме того, индуктивные фильтры часто резонируют, так что помехи на определенных частотах

могут даже увеличиться и данный фильтр может только усугубить ситуацию. Применение фильтров с потерями, которые превращают энергию паразитных сигналов в тепло, вышеуказанные проблемы не возникают. Простейшим таким фильтром является надетое на проводник ферритовое кольцо, которое на низких частотах является хорошим проводником, а на частотах 1–100 МГц его сопротивление равно 50–200 Ом и более

Так же необходимо подавлять дифференциальную помеху, проходящую по одной линии и синфазную помеху, проходящую по всем линиям. Для подавления синфазной помехи в фильтр питания добавляется синфазный дроссель. Дифференциальную помеху можно подавить стандартной LC сборкой.

Фильтрация кондуктивных помех исследуемого ШИМ-преобразователя питания производилась при помощи серийного сетевого фильтра, используемого в ОАО «Конструкторское бюро Дисплей», для фильтрации кондуктивных помех цепей питания видеомониторов. Типовая схема используемого фильтра представлена на рисунке 1.

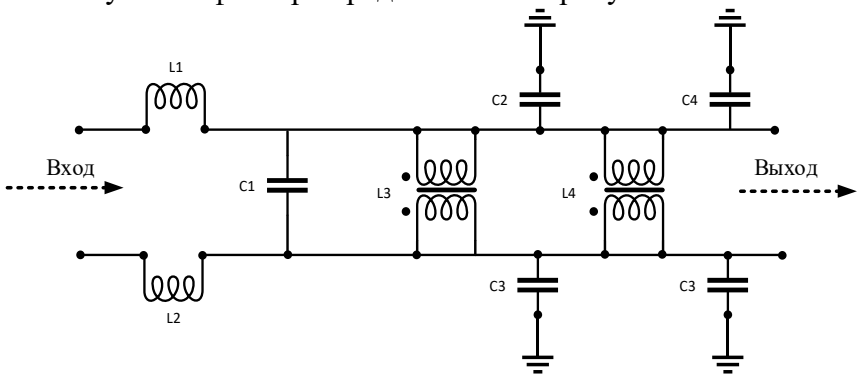


Рис. 1. Типовая схема сетевого фильтра

Данный фильтр подключался на вход ШИМ-преобразователя питания. Основная задача данного фильтра, фильтрация синфазных (за счет синфазных дросселей) и дифференциальных (за счет LC-цепочек) помех.

Экранирование. При решении задач экранирования, как только разработана структурная схема и определены необходимые уровни высокочастотных напряжений в различных ее точках, необходимо выделить цепи, чувствительные к паразитным излучениям, и возможные источники таких излучений. Обладая подобными сведениями, можно приступить к выбору материала экранов.

Коэффициент экранирования $\dot{K}_э$ представляет собой отношение напряженности электрического $\dot{E}_э$ или магнитного $\dot{H}_э$ поля в какой либо точке защищаемого пространства при наличие экрана к напряженности $\dot{E}$ или $\dot{H}$ воздействующего поля в той же точке при отсутствии экрана [2]:

$$\dot{K}_э = \frac{\dot{E}_э}{\dot{E}} \quad \text{или} \quad \dot{K}_э = \frac{\dot{H}_э}{\dot{H}}. \tag{2}$$

Волна, падающая на экран, частично отражается, а частично проходит в экран. Амплитуды обеих составляющих зависят от поверхностного сопротивления материала, из которого выполнен экран, и волнового сопротивления падающей волны. Прошедшая волна в материале экрана частично поглощается. На выходе из толщи экрана волна опять частично отражается, а частично проходит уже в экранируемую область.

Таким образом экранирующий эффект для падающих волн легко рассчитывается по формуле:

$$S\ [\text{дБ}] = R + A + B, \tag{3}$$

где R, A, B – затухание при отражении, поглощении, и внутреннем отражении соответственно, дБ [2].

Следует иметь ввиду, что установка экранов для уменьшения помех может привести к резонансам в экране, вероятность которого возрастает, когда наибольший размер экрана близок к половине длины волны излучения.

Влияние щелей и других неоднородностей экранов. Как известно, при падении на проводящий экран с прорезью волны, магнитные силовые линии поля вызывают в экране токи и, если прорезь оказывается перпендикулярно направлению наведенного тока, то на прорези возникает разность потенциалов, которая и является источником вторичного паразитного излучения экрана в пространство. Таким образом, наличие щели в экране всегда снижает его эффективность.

Заменой прорези на ряд мелких отверстий можно снизить сопротивление наведенному току, а, следовательно, и уменьшить разность потенциалов между сторонами отверстия, т. е. снизить излучения через отверстия.

Экранирование исследуемого ШИМ-преобразователя питания. Экранирование осуществлялось при помощи тонкого латуневого листа, из которого был выгнул экран. Образовавшиеся щели заклеивались алюминиевой липкой лентой. Преобразователь питания вместе с сетевым фильтром оборачивался никелевой тканью в несколько слоев, и крепко ужимался. Аплеткой экранировался соединительный кабель питания ШИМ-преобразователя и видеомонитора. На концах кабеля, оплетка была по периметру плотно прижата к никелевой ленте, являющейся экраном соответственно ШИМ-преобразователя питания и монитора. Все экраны были заземлены. Сопротивление шины заземления не более 2,5 Ом.

Заземление. Очень часто причиной тех или иных помех могут быть ошибки в заземлении, поэтому этот вопрос следует рассмотреть несколько подробнее.

Наряду с известными функциями защиты и безопасности заземляющая система должна: представлять собой цепь опорного источника напряжения; обеспечивать сигнальные и силовые цепи возврата; препятствовать появлению вблизи антенн высокочастотных потенциалов и свести к минимуму нежелательные паразитные связи между сигналами.

Протекание токов в системе заземления приводит к разности потенциалов, которая, для обеспечения нормальной работы оборудования, должна быть невелика по сравнению с амплитудой сигнала. Поэтому при проектировании системы заземления следует поддерживать импеданс заземления на как можно более низком уровне.

Чтобы снизить сопротивление связи, необходимо ограничивать размер системы заземления. Заземление различных устройств сложной системы в одной точке позволяет теоретически исключить влияние общего сопротивления заземления.

Оценка защищенности КУИ ШИМ-преобразователя СВТ. Исследования проводилась на основе методики оценки защищенности информации ШИМ-преобразователя СВТ, предложенной в соответствующей статье [5].

На рисунках 2 (Э КУИ) – 3 (ЭМ КУИ) предоставлены обнаруженные спектры исследуемых сигналов на нечетных гармониках информационного сигнала до и после внедрения пассивных методов ЗИ, описанных выше.

Анализ тонкой структуры информационных сигналов, а также внедрение схемно-конструктивных пассивных методов защиты информации позволил понизить порог обнаружения и повысить точность оценки защищенности ШИМ-преобразователя СВТ.

Рис. 2.1. Спектры 5-й и 7-й гармоник информационного сигнала

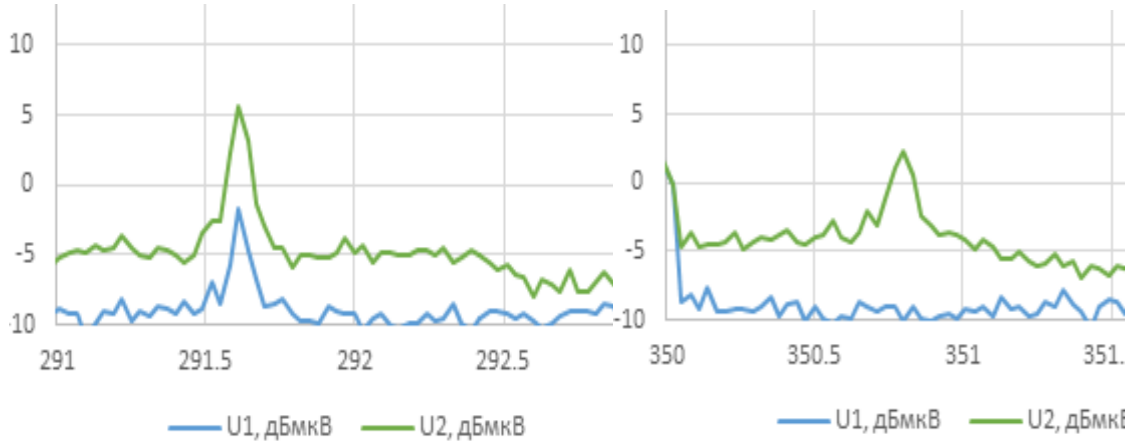


Рис. 2.2. Спектры 5-й и 7-й гармоник информационного сигнала

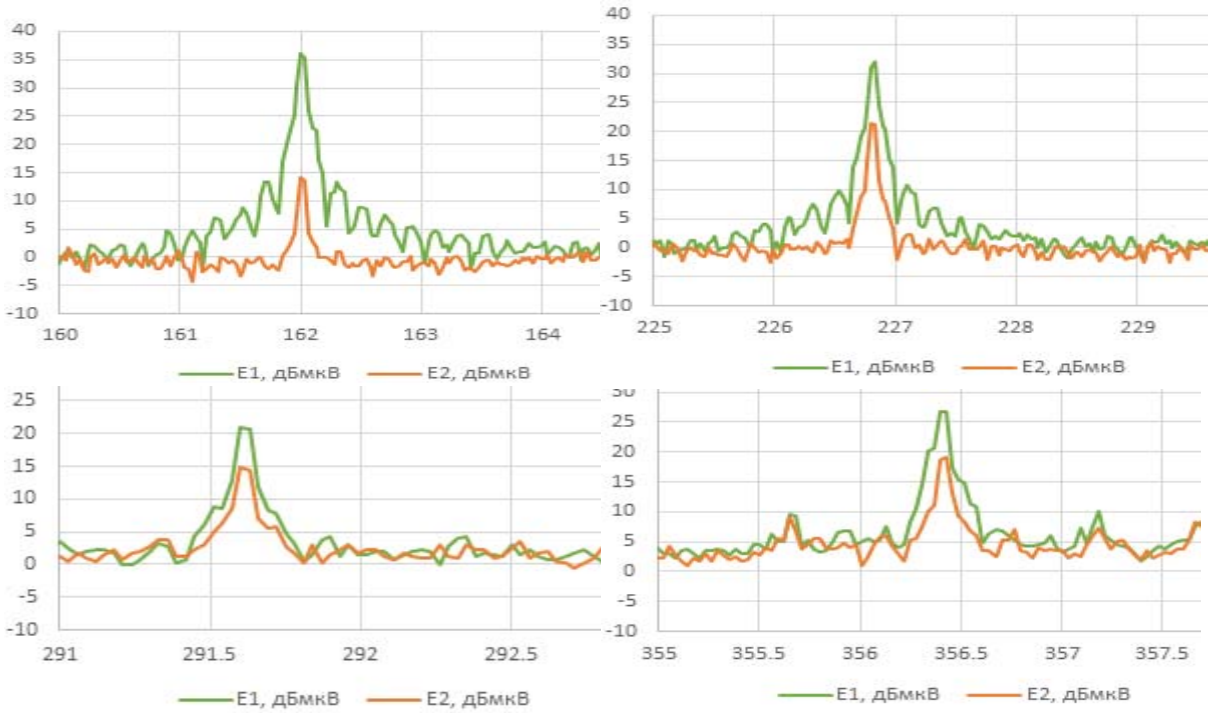


Рис. 3. Спектры 3-й, 5-й, 7-й и 9-й гармоник информационного сигнала

Список литературы

1. Железняк, В. К. Защита информации от утечки по техническим каналам : учеб. пособие / В. К. Железняк. – СПб. : ГУАП, 2006. – 188 с.

2. Князев, А. Д. Конструирование радиоэлектронной и электронно-вычислительной аппаратуры с учетом электромагнитной совместимости // А. Д. Князев, Л. Н. Кечиев, Б. В. Петров. – М. : Радио и связь, 1989. – 224 с.

3. Бузов, Г. А. Защита от утечки информации по техническим каналам : учеб. пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М. : Горячая линия – Телеком, 2005. – 416 с.

4. Уайт, Д. Электромагнитная совместимость и непреднамеренные помехи / Д. Уайт. – М. : Советское радио, 1977. – 352 с.

5. Князев, А. Д. Элементы теории и практики обеспечения электромагнитной совместимости радиоэлектронных средств / А. Д. Князев. – М. : Радио и связь, 1984.– 336 с.

УДК 621.396:621.391.037

ИНТЕЛЛЕКТУАЛЬНОЕ ПРИНЯТИЕ РЕШЕНИЙ ПО ОБНАРУЖЕНИЮ ЗАКЛАДНЫХ УСТРОЙСТВ В НЕЛИНЕЙНОЙ РАДИОЛОКАЦИИ

В.М. ЧЕРТКОВ, В.К. ЖЕЛЕЗНЯК, М.М. ИВАНОВ
Учреждение образования «Полоцкий государственный университет», г. Новополоцк, Республика Беларусь

Введение. Нелинейный радиолокатор является прибором, обеспечивающим обнаружение электронных закладных устройств (ЭЗУ). Проблема правильного обнаружения ЭЗУ с высокой вероятностью стоит достаточно остро, а ее решение является актуальной задачей. Как правило принятие решения об обнаружении ЭЗУ происходит по выявлению признаков особенных для полупроводниковых компонентов в их составе.

Основная часть. В настоящее время повышение вероятности правильного обнаружения ЭЗУ основываться на разработке методов различения объектов по двум типам – электронные (полупроводниковые компоненты РЭА) и естественные (металлические контакты и соединения, представляющие собой структуру металл-оксид-металл). Одним из информативным признаком различия является вольтамперная характеристика (ВАХ) исследуемых объектов, которая принимает квадратичный или кубический характер кривизны [1].

Авторами предложен способ распознавания типов нелинейностей [2] на основе определения характера кривизны ВАХ ЭЗУ, путем определения численных значений степенных коэффициентов полинома, аппроксимирующего его ВАХ. Разработанный способ позволяет определять и регистрировать коэффициенты полинома, аппроксимирующего ВАХ исследуемого скрытого объекта с нелинейными свойствами в выбранном направлении излучения зондирующего сигнала. Зависимости изменения степенных коэффициентов от направления и мощности излучения зондирующего сигнала позволяют сформировать идентификационный образ ЭЗУ. На рисунке 1 представлен идентификационный образ диода Д220 по квадратичному коэффициенту, где номера строк и столбцов соответствуют углу места и азимуту положения точки излучения нелинейного радиолокатора относительно исследуемого диода, а яркость соответствует числовому значению расчетного квадратичного степенного коэффициента. Аналогичным способом формируется идентификационных образ по кубическому и линейному коэффициентам полинома, который аппроксимируют ВАХ исследуемого нелинейного объекта.

Функциональная возможность идентификации ЭЗУ в известных нелинейных радиолокаторах не предусмотрена. Авторами разработан принципиально новый метод идентификации ЭЗУ. Отнесение к определенному классу распознаваемых электронных закладных устройств, возможна только при проведении нескольких серий измерений. Важным этапом получения информации о характеристиках исследуемого предполагаемого ЭЗУ с нелинейной ВАХ является распознавание типа нелинейности его элементов согласно [2]. Надежность идентификации в значительной мере будет зависеть от выбора признаков, по которым в дальнейшем они будут классифицироваться. Предложено идентификацию ЭЗУ проводить путем сравнения полученного его идентификационного образа при обследовании с эталонами идентификационных образов, хранящимися в накапливаемой базе данных [1]. Сравнение с эталонами предложено проводить путем расчета численного значения степени подобия идентификационных образов [3].

После сравнения всех записей в базе данных путем расчета числового значения критерия схожести, определяется максимально похожий идентификационный образ [4]. Если расчетное отношение превышает установленный максимальный порог, то объект классифицируется как электронное закладное устройство. Если расчетное отношение ниже установленного минимального порога, то объект классифицируется как структура металл-оксид-металл. Если расчетное отношение принимает значение от минимального до максимального порога, то объект классифицируется как неопознанный [3].

Разработан алгоритм [4], особенностью которого является построение векторов из значений разности соседних уровней для каждой гармоники и вычисление их нормы и метрики. Степень подобия определяется суммой коэффициентов корреляции соответствующих векторов гармоник и корреляции коэффициентов полинома, аппроксимирующего ВАХ [5].

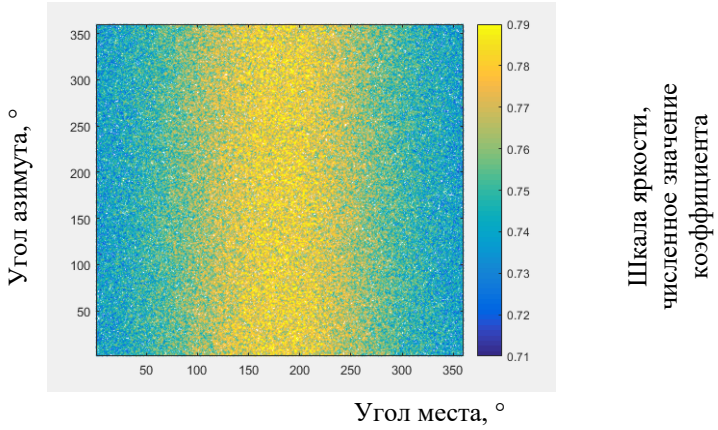


Рис. 1. Идентификационный образ по квадратичному коэффициенту эталонного диода Д220

Отличительной особенностью разработанного метода идентификации ЭЗУ является возможность применения нейронных сетей для оценки степени подобия идентификационных образов ЭЗУ. Это позволит повысить надежность идентификации и вероятность правильного обнаружения ЭЗУ и позволяет обеспечить возможность анализировать отклики от сложных зондирующих сигналов в том числе и широкополосных. Важно отметить, что применение интеллектуальных алгоритмов принятия решений на базе нейронных сетей в нелинейной радиолокации является актуальным направлением [6].

Заключение. Представлена возможность интеллектуальной идентификации ЭЗУ путем построения его идентификационного образа, который определяет зависимость изменения расчетных значений коэффициентов степенного аппроксимационного полинома от направления облучения ЭЗУ. Направление облучения ЭЗУ определяется углом места и азимутом относительно центра излучающей антенны нелинейного радиолокатора. Сформированный идентификационных образ исследуемого ЭЗУ предложено представлять в виде цветного изображения, в котором номера расположения пикселей устанавливают значения угла азимута и угла места положения точки излучения нелинейного радиолокатора относительно облучаемого ЭЗУ, а уровни яркости цветовых каналов пикселей равны значениям коэффициентов степенного полинома, аппроксимирующего ВАХ нелинейных элементов ЭЗУ. Это позволило разработать принципиально новый метод идентификации ЭЗУ, основанный на оценке степени подобия его идентификационного образа с эталонами, хранящимся в экспериментально наполненной базе данных.

В результате имитационного моделирования апробации метода идентификации ЭЗУ установлено, что вероятность правильного обнаружения (D) не ниже 0,94 для полупроводниковых компонентов РЭА и не ниже 0,84 для структур металл-оксид-металл при заданной вероятности ложного тревоги (F) для двух типов НЭ 0,01.

Список литературы

1. Чертков, В. М. Способ получения идентификационного портрета радиоэлектронных средств перехвата информации методами нелинейной радиолокации. / В. М. Чертков, В. К. Железняк // Теоретические и прикладные аспекты информационной безопасности : тез. докл. Междунар. науч.-практ. конф. (Минск, 18 мая 2017 г.) / Акад. М-ва внутр. дел Респ. Беларусь ; редкол. : А. В. Яскевич (отв. ред.) [и др.]. – Минск : Академия МВД, 2018. – С. 131–134.

2. Чертков, В. М. Определение типа нелинейности вольтамперной характеристики объекта, исследуемого нелинейным радиолокатором / В. М. Чертков, В. К. Железняк // Доклады БГУИР. – 2017. – № 8. – С. 60–66.

3. Чертков, В. М. Оценка степени подобия идентификационного портрета радиоэлектронных средств с его эталоном / В. М. Чертков, В. К. Железняк // Современные средства связи : мат-лы XXI Междунар. науч.-техн. конф., 19-20 окт. 2017 года, Минск, РБ / Белорусская государственная академия связи. – Минск, 2017. – С. 308–309.

4. Чертков, В. М. Алгоритм определения меры схожести идентификационных образов закладных устройств / В. М. Чертков, В. К. Железняк // Вестник полоцкого государственного университета. Серия С: Фундаментальные науки. – 2018. – № 4. – С. 20–27.

5. Чертков, В. М. Идентификационный портрет как основной параметр идентификации РЭС / В. М. Чертков, В. К. Железняк // Теоретические и прикладные аспекты информационной безопасности : материалы Междунар. науч.-практ. конф., Минск, 31 марта 2016 г. / Акад. М-ва внутр. дел Респ. Беларусь ; редкол.: В. Б. Шабанов (отв. ред.) [и др.]. – Минск, 2016. – С. 237–241.

6. Бельчиков, А. В. Нелинейные локаторы «ЛОРНЕТ»: инновации в каждой разработке / А. В. Бельчиков, В. С. Орлов // Защита Информации. Инсайд. – 2020. – № 1 (91).

УДК 004.056

ОПРЕДЕЛЕНИЕ УСТОЙЧИВОСТИ ОТ ВОЗБУЖДЕНИЯ ПО КРИТЕРИЮ РАУСА-ГУРВИЦА В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

С.Н. ШУСТОВСКИЙ, В.К. ЖЕЛЕЗНЯК
Учреждение образования Полоцкий государственный университет, г. Новополоцк, Республика Беларусь

Введение. Одной из основных проблем при проектировке электрических систем является задача анализа устойчивости. Электрическая цепь может выполнять свои функции, когда она устойчива. Исключением являются автоколебательные цепи, которые по определению должны быть неустойчивы на заданной частоте. Электрическую цепь можно обозначить, как устойчивую тогда, когда свободные колебания внутри затухают с течением времени. В противном случае электрическая цепь неустойчива и работает в режиме самовозбуждения внутренних контуров. Устойчивость является одним из самых важных критериев при проектировке электро- и радиоаппаратуры, содержащей усилители. В особенности важна устойчивость систем связи, как военных, так и государственных. Такая аппаратура должна быть защищена не только от внешних воздействий, но и от внутренних нежелательных процессов. Понятие устойчивости в данном случае и является защищенностью, так как при неустойчивости системы некоторая информация будет излучаться и приводить к утечке данных. При определении устойчивости существует ряд определенных сложностей. Для определения устойчивости нужно составить характеристическое уравнение системы и вычислить корни. Для цепей высокого порядка вышеперечисленные математические операции очень громоздки, а нули полиномов в аналитической форме найти принципиально невозможно [1]. Критерий устойчивости Рауса-Гурвица имеет ряд особенностей, в связи с которыми он более применим для анализа цепи высокого порядка расчетно-аналитическим методом, в отличие от критериев Михайлова, Найквиста, требующих построения сложных годографов в комплексной плоскости и произведения объемных математических операций.

Цель: показать перспективность применения метода Рауса-Гурвица при расчете устойчивости электрических цепей высокого порядка с обратной связью. Показать пример составления характеристического уравнения электрической цепи с использованием передаточной функции и обратной связи. Рассчитать устойчивость по Гурвицу в общем виде. Для облегчения определения устойчивости введем понятие передаточной функции и обратной связи, что позволит сократить количество математических операций для получения характеристического уравнения.

1. **Расчет передаточной функции.** Рассмотрим передаточную функцию на примере цепи с обратной связью, последовательной по напряжению (ОС Н-типа), представляющую собой два сложных параллельно соединенных четырехполюсника, приведенной на рис. 1.

2. Для этого типа ОС запишем равенство (1) согласно Закону напряжений Кирхгофа в операторной форме:

$$U_{вх}(p) = U_1(p) - U_{ос}(p). \quad (1)$$

Для изображения выходного напряжения запишем равенство (2)

$$U_{вых}(p) = \left[U_1(p) - U_{ос}(p)\right] H(p), \quad (2)$$

где $H(p)$ – операторная передаточная функция по напряжению.

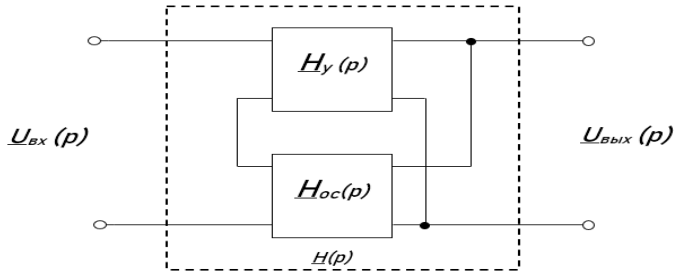


Рис. 1. Цепь с ОС Н-типа

Операторное изображение $U_{ос}(p)$ запишем через передаточную функцию ОС $H_{ос}(p)$, а напряжение $U_1(p)$ через передаточную функцию усилителя $H_y(p)$

$$U_{ос}(p) = U_{вых}(p) H_{ос}(p), \tag{3}$$

$$U_1(p) = U_{вых}(p) \times \frac{1}{H_y(p)}. \tag{4}$$

С учетом выражений (3) и (4) операторная передаточная функция по напряжению цепи (рис. 1) имеет вид: $H(p) = \frac{U_{вых}(p)}{U_{вх}(p)} = \frac{H_y(p)}{1 - H_y(p) \times H_{ос}(p)}$

Перейдем от оператора p к оператору $j\omega$, для получения комплексной передаточной функции: $H(j\omega) = \frac{U_{вых}(j\omega)}{U_{вх}(j\omega)} = \frac{H_y(j\omega)}{1 - H_y(j\omega) \times H_{ос}(j\omega)}$.

Произведение $H_y(j\omega) \times H_{ос}(j\omega) = H_p(j\omega)$ является передаточной функцией по петле ОС или петлевым усилителем.

Так же операторную передаточную функцию $H(p)$ можно представить как дробно-рациональную функцию с вещественными коэффициентами:

$$H(p) = \frac{a_n p^n + a_{n-1} + \cdots + a_1 p + a_0}{b_m p^m + b_{m-1} p^{m-1} + \cdots + b_1 p + b_0} = \frac{W(p)}{V(p)} \tag{5}$$

или

$$H(p) = H \frac{(p - p_0)(p - p_{02}) \cdots (p - p_{0n})}{(p - p_1)(p - p_2) \cdots (p - p_m)}, \tag{6}$$

где p_{01}, p_{02},..., p_{0n} – нули; p_1, p_2, ..., p_m – полюсы передаточной функции; $H = \frac{a_n}{b_m}$.

Заменив в формуле (5) оператор p на $j\omega$, получим комплексную передаточную функцию цепи: $H(j\omega) = |H(j\omega)| e^{j\varphi(\omega)}$

Для определения вида частотно зависимой ОС воспользуемся кривой, описывающей конец вектора $H_p(j\omega)$ при изменении частоты, называемой годографом (рис 2).

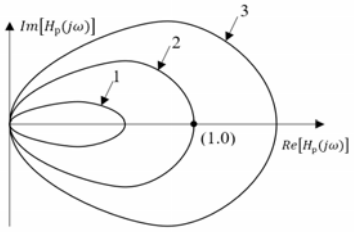


Рис. 2. Годограф ОС

Обратная связь называется положительной, если годограф $H_p(j\omega)$ лежит в правой, и отрицательной – если в левой полуплоскости комплексной плоскости. Отрицательная ОС применяется для стабилизации коэффициента усиления, подавления паразитных сигналов, коррекции частотных характеристик; положительная ОС может являться причиной неустойчивости цепи [2].

Пусть $H_{ос}$ и H_y – положительные вещественные числа. Тогда при $H_y \times H_{ос} = 1$, т. е. когда $H_{ос} = \frac{1}{H_y}$, значение передаточной функции стремится к бесконечности. Это означает, что даже при бесконечно малых значениях амплитуды входного напряжения $U_{вх}(t)$ амплитуда выходного напряжения $U_{вых}(t)$ $U_{вх}(t) = 0$ будет неограниченно возрастать. В этом случае наступает самовозбуждение цепи с ОС. Таким образом, термины неустойчивость и самовозбуждение являются синонимами.

2. Вычисление характеристического уравнения. Рассмотрим цепь с обратной связью и выведем для нее характеристическое уравнение.

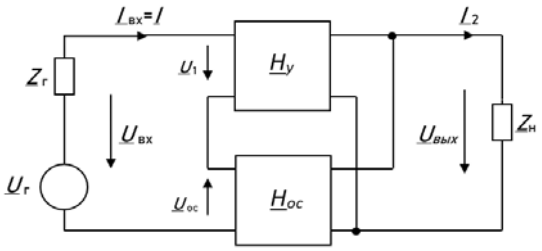


Рис. 3. Цепь с обратной связью, последовательной по напряжению

Пусть $U_{вх}(t)=0$, значит $U_{вх}(p)=0$, из рис. 3 следует: $U_{вых}(p)=\left[1-H_{ос}(p)\times H_y(p)\right]=0$. Для отрицательной и вещественной ОС согласно уравнению для коэффициента усиления усилителя, запишем:

$$H=\frac{H_y}{1+H_y\times H_{ос}} \tag{7}$$

Запишем передаточную функцию основной цепи в виде (5): $H_{ос}(p)=\frac{W_2(p)}{V_2(p)}$, $H_y(p)=\frac{W_1(p)}{V_1(p)}$. Тогда уравнение (7) перепишется следующим образом:

$$\frac{V_1(p)V_2(p)-W_1(p)W_2(p)}{V_1(p)V_2(p)}=0. \tag{8}$$

Равенство (8) выполнимо при условии: $V_1(p)V_2(p)-W_1(p)W_2(p)=0$

Так как левая часть равенства является полиномом, можно и необходимо записать ее в каноническом виде: $b_m p^m+b_{m-1}p^{m-1}+\cdots+b_1p+b_0=0$. Данное выражение является характеристическим уравнением рассматриваемой цепи.

3. Применение критерия Рауса-Гурвица. Имея характеристическое уравнение можно судить об устойчивости цепи по критерию Рауса-Гурвица.

Критерий Рауса-Гурвица относится к алгебраическим критериям устойчивости и позволяет по значениям коэффициентов b_m, b_{m-1}, b_0 характеристического уравнения, без определения его корней, узнать является ли исследуемая цепь устойчивой.

Критерий формулируется следующим образом: цепь с обратной связью является устойчивой, если полином характеристического уравнения, является полиномом Гурвица. При этом используется основное свойство полинома Гурвица: все его корни находятся в левой полуплоскости комплексной переменной p. [1]

Для того чтобы многочлен $b_m p^m+b_{m-1}p^{m-1}+\cdots+b_1p+b_0=0$ являлся полиномом Гурвица, необходимо и достаточно, чтобы были положительными определитель Рауса–Гурвица (9)

$$D_{n-1}=\begin{bmatrix} b_{m-1} & b_{m-3} & b_{m-5} & \cdots & 0 \\ b_m & b_{m-2} & b_{m-4} & \cdots & 0 \\ 0 & b_{m-1} & b_{m-3} & \cdots & 0 \\ 0 & b_m & b_{m-2} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & b_0 \end{bmatrix} \tag{9}$$

и все главные миноры этого определителя.

В первой строке записываются коэффициенты полинома Гурвица через один, начиная со второго. Во второй строке они записываются через один, начиная с первого. Вторая пара строк формируется путем смещения первой пары строк на одну позицию. Третья пара – смещением второй пары строк еще на одну вправо и т. д.

Если все n-1 главных миноров Гурвица положительны, а минор n-го порядка равен нулю: $\Delta n=0$, то система находится на границе устойчивости.

Таким образом расчет устойчивости цепи сводится к простому решению матрицы Гурвица, а основные затруднения может вызвать только лишь составление характеристического уравнения и определение вида ОС.

Заключение

1. Устойчивость цепи, вычисленная по критерию Рауса-Гурвица дает понятие о защищенности информации, так как устойчивая цепь не будет излучать сигналы, приводящие к утечке данных.

2. Метод Рауса-Гурвица применим для вычисления цепей любого порядка, что немаловажно при проектировании сложной аппаратуры связи.

3. Метод пригоден для анализа схем двойного назначения с разными параметрами элементов.

4. Так как вычисление устойчивости сводится к решению матрицы, возможно применить компьютерные методы вычисления, что позволит автоматизировать процесс

5. Метод позволяет определить запас устойчивости цепи, что довольно важно при проектировании оборудования, работающего в условиях влияния на него извне высокочастотных помех и импульсов.

Список литературы

1. Шамриков, Б. М. Основы теории цифровых систем управления : учебник для высш. техн. учеб. завед. / Б. В. Шамриков. – М. : Машиностроение, 1985. –С. 69–82.

2. Гуревич, И. В. Основы расчетов радиотехнических цепей (линейные цепи при гармонических воздействиях) / И. В. Гуревич. – Изд. 3-е, испр. и доп. – М. : Связь, 1975. – С. 25–36.

УДК 004.052.2

ОЦЕНКА СТАБИЛЬНОСТИ ПОЛУЧЕНИЯ ИНФОРМАЦИИ БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТОМ ПОД ВЛИЯНИЕМ ПУЛЬСАЦИОННОЙ СОСТАВЛЯЮЩЕЙ ВЕТРОВОГО ДАВЛЕНИЯ

В.К. ЖЕЛЕЗНЯК А.И. ЯРИЦА, А.В. КАРЛА
Полоцкий государственный университет,
г. Новополоцк, Республика Беларусь

Для поддержания нужной высоты, стабильности равномерного расположения летательного аппарата по координатным осям требуется учитывать многие воздействующие факторы. Часть из них рассмотрены в работе [1]. В данной работе дана оценка стабильности получения информации БЛА под влиянием постоянной и пульсационной составляющих ветрового давления.

При рассмотрении расстояния при принятии сигнала, следует отметить такой фактор, как влияние атмосферы на точность координат БЛА. Движение масс воздуха в атмосфере относительно земной поверхности происходит под воздействие разности атмосферного давления, определяемого барическим градиентом, силой трения, отклоняющей силой вращения Земли (сила Кориолиса) и центробежной силой. Сила трения частиц воздуха о поверхность земли отклоняет направление ветра от прямолинейного, но сказывается только в нижних сотнях метрах. С ростом высоты над поверхностью земли влияние силы трения уменьшается, что приводит к повышению скорости ветра. Наиболее распространена степенная зависимость скорости ветра с высотой:

$$V_z = V_\phi (\mathrm{z}/\,\mathrm{z}_0)^\alpha \tag{1}$$

и логарифмическая

$$V_z = V_\phi \frac{\ln z / z_0}{\ln z_\phi / z_0} \tag{2}$$

где V_ϕ – скорость ветра на высоте флюгера или измерительного прибора; z – высота над поверхностью земли; z_ϕ – высота флюгера или другого прибора, чаще всего около 10 м; z_0 – параметр шероховатости (условной) поверхности или высота, на которой скорость равна нулю; α – показатель, принимаемый равным 0,08–0,4.

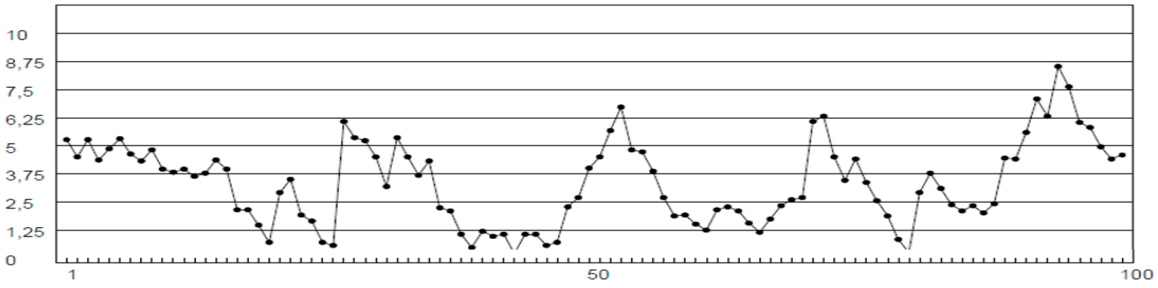


Рисунок 1. График изменения скорости ветра. Период 100 секунд

При значительных кратковременных отклонениях от средней величины скорости ветра говорят о шквалистости ветра [2]. Порывистость в исследованиях характеризуют с помощью средних квадратов пульсации (порывов) составляющих скорости ветра и стандартных отклонений. Порывы ветра характеризуются коэффициентом порывистости, являющимся отношением наибольшей скорости в порыве к средней за определенный промежуток времени (рис. 1). Коэффициент порывистости убывает с увеличением средней скорости ветра (рис. 2).

Неупорядоченный хаотический характер пульсаций скорости ветра в приземном слое позволяет считать, что распределение пульсаций скоростного напора следует нормальному закону распределения Гаусса. Тогда добавка к скоростному напору, учитывающая порывистость, может быть определена из записей мгновенной скорости ветра в характерных районах, если средние величины скорости ветра во время наблюдений были достаточно большие.

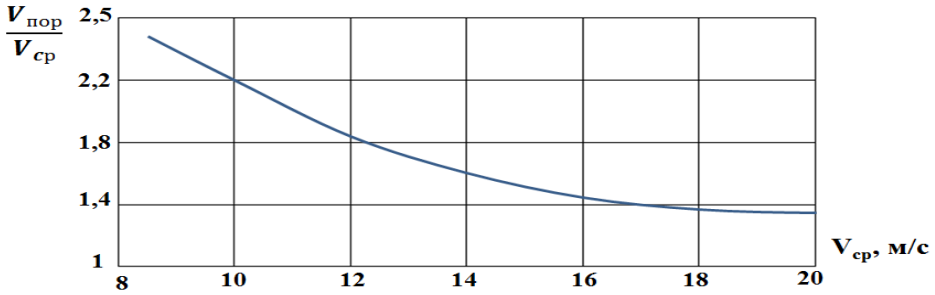


Рис. 2. Коэффициент порывистости в зависимости от средней скорости ветра

Сама природа ветра, когда на среднюю скорость накладываются порывы ветра (рисунок 3), указывает на то, что основную ветровую нагрузку следует определять, как сумму средней (статической) и пульсационной (динамической) составляющих:

$$w = w_m + w_p \tag{3}$$

Значение средней составляющей ветровой нагрузки в зависимости от эквивалентной высоты над поверхностью земли следует определять по формуле:

$$w_m = w_0 \cdot k(z_e) \cdot \mathrm{c} \tag{4}$$

Наличие в ветровом потоке сдвига и пульсаций скорости еще более усложняет ситуацию, приводя к дополнительным нестационарным воздействиям. Значение пульсационной составляющей ветровой нагрузки определяется по формуле:

$$w_p = w_m \zeta(z_e) v \ , \tag{5}$$

Проанализируем ее более подробно.

- w_m – средняя составляющая ветровой нагрузки, определяется по формуле 2.6;
- ζ – коэффициент пульсации давления ветра, принимаемый для эквивалентной высоты z_e;

Коэффициент пространственной корреляции пульсаций давления v следует определять для всей расчетной поверхности беспилотного летательного аппарата или его отдельной конструкции, для которой учитывается корреляция пульсаций [2]. \\\\\

Для оценки воздействия пульсационной составляющей ветрового давления, проведены измерения скорости ветра, влажности воздуха и температуры [3]. Измерение этих показателей проводились высокоточным анемометром марки Мегеон – 1107 (табл. 1).

Таблица 1

Технические характеристики прибора

Диапазон измерений потоков воздуха	Разрешение измерений потоков воздуха	Диапазон измерений температуры	Подключение к компьтеру	Погрешность измерений температуры	Наличие дисплея
0,3–20 м/с	0,01 м/с	0–50 ◦C	USB	±0,5 ◦C	есть

Измерения проводились в городской застройке, с наветренной стороны стандартного прямоугольного жилого дома высотой 40 м. Результаты представлены в таблице 2**.**

Таблица 2

Измерение скорости ветра

№ измерения	Температура, ◦С	Влажность воздуха, %	Скорость ветра, м/с	Время измерения
1	13,5	64,5	0	19:41:11
10	13,5	64,5	8,08	19:41:20
20	13,5	64,5	4,19	19:41:30
…	…	…	…	…
99	13,5	64,5	2,75	19:42:29
100	13,5	64,5	2,34	19:42:30

График изменения скорости изображен на рисунке 3.

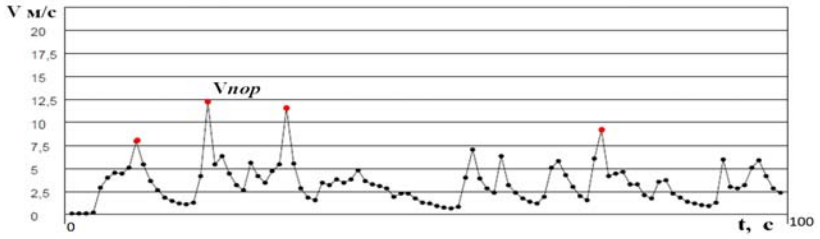


Рис. 3. График изменения скорости ветра за 100 секунд

В результате статистической обработки измерений, получаем среднее математическое ожидание скорости ветра $V_{ср}$ = 3,3 м/с. Максимальная скорость ветра $V_{пор}$ = 12,3 м/с.

Плотность воздуха при нормальном барометрическом давлении (760 мм рт.ст.) и температуре 15 ^{0}С равна 1,25 кг/м^3. Состояние воздуха при таком давлении и температуре принимается за стандартную атмосферу. в ходе расчетов получили w_o = 0,068 кПа.

Средняя составляющая ветровой нагрузки:

$$w_m = w_0 \cdot k(z_e) \cdot \mathrm{c} = 0,068 \cdot 1,1 \cdot 0,8 = 0,06$$

Пульсационная составляющая ветровой нагрузки:

$$w_p = w_m \zeta(z_e) v = 0,06 \cdot 0,8 \cdot 0,59 = 0,03$$

Основная ветровая нагрузка, учитывающая среднюю составляющую и пульсационную, составила 0,09 кПа или 9,2 кг·с/м^2. При максимальной скорости ветра ветровая нагрузка составила 0,12 кПа или 12,2 кг·с/м^2

В ходе системного анализа ветрового давления выделены основные ключевые моменты, которые нужно учитывать при подготовке, проведении и обработки результатов измерений. Требуется измерить, помимо скорости ветрового потока, температуру, влажность и атмосферное давление, так как три этих составляющих оказывают влияние на плотность воздушной струи. При их повышенных значениях, удельный вес воздуха становится больше, соответственно, возрастает величина переносимой энергии и, как следствие, увеличивается ветровая нагрузка, оказываемая на беспилотные летальные аппараты. Также ветровая нагрузка имеет зависимость к усилению от увеличения высоты. Так при скорости ветра равной 20 м/с, расчетные значения ветровой нагрузки в первом приближении на высоте 10 м будут примерно равны 0, 18 кПа, на высоте 20 м – 0,28 кПа, а на высоте 30м – 0,36 кПа. Пульсационная составляющая в короткий период времени (1–2 секунды) повышает ветровое давление более чем на 30 %.

Список литературы

1. Карла, А. В. Оценка стабильности получения информации от параметров установленных датчиков / А. В. Карла, В. К. Железняк // Вестник Полоцкого государственного университета. Серия С, Фундаментальные науки. – 2020. – № 12. – С. 30–35.

2. Ярица, А. И. Оценка воздействия на точность определения координат точки приема сигналов спутниковой системы точного позиционирования при динамических ветровых нагрузках / А. И. Ярица // Вестник Полоцкого государственного университета. Серия С. Фундаментальные науки. – 2018. – № 4. – С. 38–44.

3. Железняк, В. К. Методика математической обработки в оценке ветровых нагрузок на точку приема и передачи сигналов, расположенную на поверхности здания / В. К. Железняк, А. И. Ярица, С. В. Лавров // Современные средства связи : мат-лы XXIII Междунар. науч.-техн. конф., 18–19 октября 2018 г. / Бел. гос. акад. Связи ; редкол. : А. О. Зеневич [и др.]. – Минск, 2018.

УДК 681.586

ОБЗОР ДАТЧИКОВ ДЛЯ ОБНАРУЖЕНИЯ ИНВАЗИВНЫХ АТАК

И.М. МАРКИН
Московский физико-технический институт
(национальный исследовательский университет), г. Долгопрудный, Российская Федерация

Введение. В наше время почти вся информация так или иначе храниться в цифровой среде на различных устройствах. В связи с этим возникает необходимость защищать данные устройства от большого количества разных атак, целями которых являются кража или повреждение информации.

По способу доступа к объекту атаки делятся на инвазивные и неинвазивные. Неинвазивными атаками называются атаки на различные устройства, которые используют только информацию и данные, доступные извне, то есть не требуют физического доступа к устройству и могут быть проведены удаленно. Инвазивными атаками называются атаки, осуществляемые путем физического доступа к устройству для получения различного рода информации.

Обнаружение инвазивных атак осуществляется с помощью мониторинга состояния объекта. Состояние объекта должно постоянно отслеживаться путем считывания показаний имеющихся у объекта датчиков для того, чтобы при выходе показаний датчиков за пределы допустимых значений, предпринять меры по изменению режима работы на более безопасный [1-3]. Однако, какие именно датчики должны использоваться для достижения этой цели? Ответ на данный вопрос является целью данной статьи. Мониторинг состояния объекта включает в себя мониторинг напряжения питания, механизм обеспечения безопасного тактирования и обнаружение физического доступа [4], который подразумевает под собой возможность детектирования вскрытия корпуса прибора и принятия мер для смены режима работы на безопасный или уничтожения чувствительной информации.

Все датчики, которые рассматриваются в данной работе потребляют энергию, поэтому логичный шаг, который необходимо предпринять злоумышленнику при проведении инвазивной атаки, – обесточить устройство, тем самым лишив питания датчиков, благодаря которым происходит обнаружения инвазивных атак. Для того, чтобы этого не произошло, необходимо использовать источники бесперебойного питания, которые способны обеспечивать устройство и датчики питанием до тех пор, пока не будут произведены необходимые действия по переходу в безопасный режим. После этого датчики могут продолжать работу до полной разрядки источника бесперебойного питания или перейти в спящий режим с целью энергосбережения.

Глава 1. Инвазивные атаки с вскрытием корпуса. Инвазивные атаки, осуществляемые зондированием кристалла, шлифованием, резкой, травлением и ионным травлением кристалла, на данный момент являются теми атаками, защите от которых некоторые производители микросхем уделяют отдельное внимание. Все эти атаки объединяет одно общее требование – необходимость вскрытия или повреждение корпуса устройства с целью получения доступа к микросхемам.

Для обнаружения данного типа атак необходимы датчики, которые способны отслеживать вскрытие и//или повреждение корпуса устройства. Таковыми датчиками являются группа датчиков перемещения и усилий, способные отслеживать факт вскрытия корпуса устройства или, в некоторых случаях их попытки. Существует классификация по физическому принципу действия, которая применима к каждому типу датчиков (рис. 1) [5].

Большинство датчиков перемещения и усилий хоть и имеют свои особенности, обусловленные физическим принципом действия, но способны отлавливать лишь перемещение крышки корпуса устройства, поэтому большинство из них в данной работе рассматриваться не будут. В данной работе будут рассмотрены наиболее популярные типы датчиков.

Самый популярный тип датчиков, используемых для обнаружения инвазивных атак со вскрытием корпуса – это тамперы. Тампер является разновидностью резистивных датчиков, а именно электромеханическим датчиком, поскольку преобразует перемещение первичного объекта (замыкание контакта) в скачкообразное изменение сопротивления электрической цепи постоянного или переменного тока. Другими словами, тампер – это контакт, находящийся под крышкой устройства и срабатывающий при снятии последней. В некоторых датчиках данного типа присутствует дополнительный, второй контакт, реагирующий на отрывание устройства от места фиксации. Тамперы широко используются в различных устройствах благодаря дешевизне, простоте конструкции и легкости установки [6].

Рис. 1. Классификация датчиков перемещения и усилий

Еще одним популярным типом датчиков являются фотоэлектрические датчики или фотодатчики. Данный тип датчиков, в отличие от тамперов, способен отследить не только вскрытие крышки корпуса устройства, но и нарушение его целостности (возникновение отверстий). Однако для нормального функционирования фотоэлектрических датчиков необходим полностью закрытый корпус, не пропускающий световые лучи от других источников, что может являться минусом в некоторых случаях. Фотодачики бывают следующих типов: фотоспоротивление, фотодиод с p-n переходом, PIN-фотодиод и фототранзистор. Каждый из этих типов имеет особенности, обусловленные принципом действия, и являются представителями различных ценовых категорий. Так датчики на основе фотосопротивления имеют большее значение отклика, однако имеют хорошую точность измерений и слабо зависят от состояния окружающей среды. В свою же очередь фотодиоды обладают малым временем отклика, но не могут похвастаться независимостью измерений от других факторов. Фототранзистор точен и слабо подвержен влиянию среды, однако его отклик не является линейной величиной. Некоторые представители различных фотодатчиков представлены в таблице ниже [7].

Таблица 1

Некоторые представители упомянутых типов фотодетекторов

Прибор/Изготовитель	Тип	Спектральный диапазон	Время отклика
VT935G / «EG&G Вактек»	Фотосопротивление	550 нм	5–35 мс
SFH213 / «Сименс»	Si p-n	850 нм	5 нс
BPX65/»Синтроник»	Si PIN	850 нм	3,5 нс
BPV1I / TFK	Фототранзистор	950 нм	3,8 мкс

Стоит отметить один из серьезных недостатков данных датчиков. Фотодатчики не способны корректно работать в среде со световым «шумом», то есть при наличии периодических световых сигналов в корпусе устройства. Таковым «шумом» может являться мигание диодов основного устройства. Еще одним недостатком является возможность атаки, при которой во время открытия устройства на светодиод не падает световые лучи, другими словами «атаки в темноте», в результате чего светодиод может не отследить начало инвазивной атаки.

Следующие типы датчиков хоть и не имеют широкого распространения, но заслуживают упоминание в виду их особенностей. Датчикам давления в отличие от фотодатчиков для обнаружения инвазивной атаки необходима не просто закрытость корпуса, а его полная герметичность. При вскрытии корпуса давление внутри корпуса изменится, в результате чего сработает датчик. Существует разные подтипы датчиков с различными характеристиками и чувствительностями.

И последний тип датчиков, заслуживающий упоминания, – ультразвуковые датчики перемещения. Принцип работы данных датчиков основан на взаимодействии ультразвуковых колебаний с измеряемой средой с помощью фиксации отраженной от объекта ультразвуковой волны. Кроме того, ультразвуковые приборы могут применяться для точного измерения толщины различных материалов без нарушения их целостности. Еще ультразвуковые датчики имеют такие плюсы, как низкая погрешность, высокая надежность и независимость от температуры. Однако данные датчики не смогут исправно работать в средах с большим уровнем шума и вибрациями. То есть, такие датчики нежелательно устанавливать в местах, подверженных вибрации. Например, если рассматривать корпус персонального компьютера, то сильно шумящие вентиляторы могут помешать нормальному функционированию ультразвуковых датчиков [5].

Также стоит упомянуть еще один способ обнаружения инвазивной атаки, осуществляемой с помощью вскрытия корпуса устройства. Однако, данный способ более подходит не к микросхемам, а к большим объектам, таким как банковские аппараты или персональные компьютеры. Видеокамеры имеют ряд возможностей, которыми не обладают другие датчики. Благодаря видеофиксации возможен просмотр всего процесса инвазивной атаки, благодаря которому возможно определить личность, совершающую инвазивную атаку, и способ проведения этой атаки. Сегодня этот способ является одним из самых распространенных способов обнаружения инвазивной атаки.

Глава 2. Инвазивные атаки с использованием экстремальных температур. Рассмотрим следующий тип инвазивной атаки на устройства, который использует изменение температуры устройства. Один из таких способов – cold boot attack. В основе данного типа атак используется эффект сохранения данных в ОЗУ типа DRAM и SRAM после выключения питания. Данные частично сохраняются в течение периода от нескольких секунд до минут. Однако с помощью охлаждения до температуры ниже -50 °C данные могут сохраняться дольше [8]. Другой возможный способ инвазивной атаки заключается в использовании высокой температуры для повреждения корпуса или микросхемы. Это может быть концентрированная серная кислота, разогретая до 300 градусов Цельсия, с помощью которой возможно растворение корпуса устройства, или обычный сварочный аппарат, который может использоваться для тех же самых целей. Инвазивные атаки с использованием экстремальных температур также являются инвазивными атаками со вскрытием корпуса, поэтому она может быть обнаружена датчиками перемещения и усилий. Однако не все датчики способны исправно работать при экстремальных температурах, в связи с чем появляется необходимость отслеживать возникновение подобных температур.

Датчики, способные отслеживать инвазивные атаки, осуществляемые с помощью высоких или низких температур, называются термодатчиками. Существует несколько подтипов данных датчиков, которые имеют те или иные особенности, но в данной работе будет акцентировано внимание на четырех типах температурных, датчиков наиболее используемых и пригодных для обнаружения инвазивной атаки – термопары, терморезисторы, полупроводниковые и акустические.

Термопара – этот датчик, принцип действия которого основан на разнице температур, представляет собой два проводника из разных металлов, спаянные в одной точке, в которой

измеряется температура и сравнивается с температурой свободных, так называемых «холодных», концов, находящихся при постоянной температуре. Преимущества термопар – большой температурный диапазон измерения (от –200 °C до +1000 °C), а недостатками являются невысокая точность и необходимость вносить поправку на температуру «холодного» конца.

Терморезисторы являются датчиками для измерения температуры, принцип действия которых основан на зависимости электрического сопротивления от температуры. Они имеют как преимущества, так и недостатки перед термопарами. Плюсами являются более высокая точность измерения и стабильность, практически линейная характеристика, и отсутствие необходимости компенсации холодного спая. Минусами же являются малый диапазон измерений (большинство измеряет температуру от –10 °C до +70 °C, но существуют варианты с диапазоном от –50 °C до +125 °C).

Полупроводниковые термодатчики работают на принципе изменения характеристик p-n перехода под воздействием температуры. Несомненными плюсами такого решения является дешевизна, высокая точность данных, и линейность характеристик на всем диапазоне измерения. Однако, данному подтипу характерен малый диапазон температуры (от –50 °C до +150 °C). Принцип работы акустических термодатчиков основан на разнице скорости звука в среде при разной температуре. Это бесконтактный метод, позволяющий измерять температуру от –270 до +1100 °C в закрытых полостях, а также в среде, недоступной для прямого измерения [1].

Глава 3. Атаки по ошибкам вычислений. Атаки по ошибкам вычислений также носят инвазивный характер. Основная идея заключается в осуществлении различных воздействий на шифратор с целью создания искажения информации на некоторых этапах шифрования. Управляя этими искажениями и сравнивая результаты на разных этапах работы устройства, криптоаналитик может восстановить секретный ключ. Например, можно попытаться поменять состояние внутреннего регистра или ячейки памяти, спровоцировать сбой при выполнении криптографической операции или записи в EEPROM. Инструментами для проведения таких атак служат, например, импульсная многолучевая лазерная установка, FIB или просто генератор импульсных помех.

Поскольку некоторые методы осуществления инвазивной атаки по ошибкам вычислений подразумевают непосредственный доступ к микросхемам, то обнаружив вскрытие или повреждение корпуса с помощью датчиков, описанных ранее (фотодатчиков, тамперов, магнитно-механических датчиков и ультразвуковых датчиков), возможно обнаружить данный тип атаки.

Еще один способ атаки по ошибкам вычисления – атака с помощью изменения напряжения питания устройства для нарушения его нормального функционирования [3]. Для мониторинга напряжения питания используются аналого-цифровые преобразователи (далее АЦП), которые преобразуют входной аналоговый сигнал (напряжение) в цифровой код. Существует несколько основных групп АЦП, разделенных по принципу работы: параллельные АЦП, АЦП с двойным интегрированием, АЦП с обратной связью. У каждой из них свои достоинства и недостатки. Таблица сравнения различных АЦП представлена ниже. Как видно из таблицы АЦП с обратной связью является золотой серединой между быстрыми параллельными АЦП и точными АЦП с двойным интегрированием.

Таблица 2

Сравнение различных типов АЦП

Аналого-цифровой преобразователь	Цена	Скорость
Параллельный	Высокая	Очень высокая (30 нс)
С обратной связью	Выше средней	Высокая (от 25мкс до 400 нс)

Существуют способы осуществления инвазивной атаки по ошибкам вычислений, не требующие вскрытия корпуса. Одним из методов проведения подобной атаки является инжекция помех – использование переменного магнитного поля для создания помех. С помощью воздействия переменного магнитного поля на устройство, в цепях устройства возникают вихревые токи, которые способны изменять состояния ячеек памяти. Также с помощью данного метода возможно перевести устройство в некорректный режим работы,

способный дать атакующей стороне дополнительную информацию о режимах работы устройства [3]. Для обнаружения подобного типа атак возможно использовать датчики Холла и датчики Виганда, которые принадлежат группе магнитно-механических датчиков.

Атака на тактовую частоту микроконтроллера также является инвазивной атакой по ошибкам вычислений. Смысл атаки на тактовую частоту не сильно отличается от остальных атак по ошибкам вычислений. С помощью данной атаки можно управлять отклонением тактовый частоты от заданного нормы и тем самым добиться полного изменения выполнения инструкций в устройстве, вплоть до невыполнения определенной инструкции.

Механизм обеспечения безопасного тактирования (подобный элемент присутствует в линейке микроконтроллеров STM32, где называется CSS – clock security sistem) обеспечивает безопасное переключение тактовых частот различных источников. Принцип работы механизма обеспечения безопасного тактирования заключается в следующем: при запуске внешнего тактирующего генератора включается детектор частоты, который при сбое внешнего генератора (даже если он не является источником системной частоты) сразу же выключает данный генератор, включает внутренний тактирующий генератор, устанавливает его источником системной частоты, посылает сигнал ошибки системной частоты расширенным таймерам и генерирует прерывание, извещая программу о сбое во внешнем тактирующем генераторе. Таким образом, с помощью механизма обеспечения безопасного тактирования происходит обнаружение и защита от инвазивной атаки [1].

Заключение. В данной работе был рассмотрен мониторинг состояния устройства, который осуществляется благодаря считыванию информации с различных датчиков, имеющихся у данного устройства, как способ обнаружения инвазивных атак на различные устройства, такие как микросхемы, банкоматы или персональные компьютеры. Для обнаружения различных способов инвазивных атак используются различные датчики:

- группа датчиков перемещения и усилий (обнаруживают вскрытие корпуса устройства);
- датчики температуры (отслеживают инвазивные атаки с помощью экстремальных температур);
- датчики Холла и Виганда (отслеживают атаки по ошибкам вычислений с помощью переменного магнитного поля);
- Тамперы (определяют перемещение устройства с места фиксации);
- Аналого-цифровые преобразователи (фиксируют атаки по цепям питания);
- CSS (используется для обнаружения атак на тактовую частоту).

Для обнаружения одной и той же атаки в некоторых случаях подходят различные виды датчиков. Выбор того или иного датчика зависит от его характеристик и условий, в которых он будет использоваться. Для увеличения эффективности обнаружения инвазивных атак на устройство необходимо одновременно использовать несколько различных типов датчиков, отвечающих за обнаружение различных видов инвазивных атак. Например, использование фотодатчиков вместе с датчиком Холла и датчиком температуры способны обнаружить большинство инвазивных атак.

Список литературы

1. Моц, М. Кибербезопасность на уровне микроконтроллеров / М. Моц // Control Engineering Россия. – 2019. – № 83. – С. 70–74.

2. Мытник, К. Я. Смарт-карты и информационная безопасность / К. Я. Мытник, С. П. Панасенко. – М. : ДМК Пресс, 2019. – 516 с.

3. Емельянов, М. Средства противодействия угрозам безопасности в микроконтроллерах STM32G0 [Электронный ресурс]. – Режим доступа : https://www.compel.ru/lib/131887. – Дата обращения : 11.05.2021.

4. Иго, Т. Arduino, датчики и сети для связи устройств / Т. Иго. – 2-е изд. – СПб. : БХВ-Петербург, 2015. – 544 с.

5. Зудин, В. Л. Датчики: измерение перемещений, деформаций и усилий : учеб. пособие для вузов. – 2-е изд. – М. : Издательство Юрайт, 2020. – 199 с.

6. Немного теории. Тампер. [Электронный ресурс]. – Режим доступа : https://www.easy-ops.ru/nemnogo-teorii/tamper. – Дата обращения : 11.05.2021.

7. Джексон, Р. Г. Новейшие датчики / Р. Г. Джексон. – М. : Техносфера, 2007. – 384 с.

8. Cool Boot Attack: вспомнить все. 2008 [Электронный ресурс]. – Режим доступа : https://xakep.ru/2008/02/28/42561/. – Дата доступа : 11.05.2021.

УДК 004.056.5

КОМБИНИРОВАННЫЙ МЕТОД ФОРМИРОВАНИЯ КРИПТОГРАФИЧЕСКОГО КЛЮЧА С ПОМОЩЬЮ СИНХРОНИЗИРУЕМЫХ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

М.Л. РАДЮКЕВИЧ, В.Ф. ГОЛИКОВ
Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации», г. Минск, Республика Беларусь
Белорусский национальный технический университет, г. Минск, Республика Беларусь

Введение. Одной из важных задач современной криптографии является формирование общего криптографического ключа у абонентов, обменивающихся информацией через открытый для прослушивания канал связи. В более общей постановке говорят о формировании общего секрета, подразумевая под ним некое число.В работе [1] предлагался способ формирования общего секрета путем создания частично совпадающих бинарных последовательностей (БП) с последующим устранением несовпадающих битов. В двух БП, формируемых случайным образом независимо друг от друга, относительное количество несовпадающих битов является случайной величиной с математическим ожиданием $M\left[\frac{n_{ns}}{N}\right]=0,5$, где n_{ns} – количество несовпадающих битов, N – длина БП в битах. Величина $\delta=\frac{n_{ns}}{N}$ получила название доля несовпадающих битов.

Под частично совпадающими БП понимаются БП, у которых математическое ожидание доли несовпадающих битов δ не равно 0,5. БП, у которых $M[\delta]=0,5$ являются статистически независимыми и не могут быть согласованы никаким методом [2], так как при этом раскрываются все биты согласуемых последовательностей. Основной проблемой описанного способа является задача формирования БП со свойствами частично совпадающих БП. Метод, который был реализован при этом, как выяснилось в дальнейшем исследовании, оказался уязвим к атаке, основанной на вычислении некоторой части битов путем выдвижения гипотез о их значениях и уточнении вероятностей этих гипотез в процессе итерационного согласования [1]. Причем оказалось, что увеличение совпадений, приводит к уменьшению конфиденциальности формируемого секрета. Кроме того, серьезным недостатком была необходимость создания большого начального числа битов в исходных последовательностях для получения итоговой последовательности размером в десяток битов.

В связи с изложенным представляет интерес разработка комбинированного способа формирования общего секрета, в котором в качестве первого этапа (этапа формирования частично совпадающих БП) используются синхронизируемые искусственные нейронные сети (СИНС). Использование СИНС для формирования общего криптографического ключа предложено В. Кантером, И. Кинцелем и описано в [3-10].

1. Базовый алгоритм. Первый этап – формирование частично совпадающих БП. Пусть абоненты A и B, имеют СИНС со структурой и параметрами, описанными в [11]. Подавая на входы своих сетей случайную последовательность $\vec{x}(t)$, и обмениваясь выходными величинами $Z^{A/B}(t)$, где t – номер такта синхронизации $(t=1,2,3,...)$, A и B такт за тактом сближают секретные вектора весовых коэффициентов (ВК) своих сетей, т. е. $\vec{W}^{A}(t)\Leftrightarrow\vec{W}^{B}(t)$. Процесс останавливается на некотором такте d, при котором вероятность совпадения ВК у сетей A и B гарантированно ниже чем 1, т. е. синхронизация является досрочно прерванной. При этом, поскольку изначально вектора ВК сетей формировались случайно с равномерным законом распределения и независимо друг от друга, то

математическое ожидание доли несовпадающих битов было равно $M[\delta]=0,5$, а в момент остановки синхронизации станет $0,5<M[\delta]<1$. Величину d следует выбирать из компромиссных соображений, имея ввиду, что чем больше d, тем меньше n_{ns} и тем меньше итераций потребуется для окончательного согласования БП на втором этапе.

Второй этап-устранение несовпадающих битов. Этап заключается в преобразовании векторов ВК $\vec{W}^A(d)$ и $\vec{W}^B(d)$ в БП $S^A(d)$ и $S^B(d)$ в соответствии с [11]. В [1] показано, что если БП имеют математическое ожидание доли несовпадающих битов $M[\delta]\le 0,2$, то число необходимых итераций не превышает 3. При этом длина итоговой БП по сравнению с начальной уменьшается как минимум в 2^l раз, где l – число итераций. Таким образом вся процедура предлагаемого метода составляет d тактов синхронизации и l тактов фильтрации несовпадений.

Если способ согласования частично совпадающих БП подробно рассмотрен в [1], то вопросы, связанные с выбором параметров сетей и параметров процесса синхронизации требуют обоснования и расчета.

Очевидно, что принимаемые решения зависят не только от действий A и B в процессе синхронизации, но и от возможных действий криптоаналитика Е, прослушивающего канал связи и владеющего всей обменной информацией, за исключением значений ВК сетей. Таким образом, необходимо выявить возможные уязвимости предлагаемого метода, оценить их опасность и провести коррекцию базового метода с целью обеспечения требуемой конфиденциальности формируемого общего секрета.

2. Возможные уязвимости базового метода и методы их устранения. На наш взгляд, предлагаемый метод может быть атакован как на первом так и на втором этапах. На первом этапе , т. е. при синхронизации сетей A и B, криптоаналитик E создает свою сеть, идентичную сетям A и B за исключением начальных значений ВК, синхронизирует (в дальнейшем будет рассматриваться только геометрическая атака, как наиболее эффективная) свою сеть с сетью, например, A в надежде, что его сеть успеет полностью синхронизоваться за отведенное число тактов d. В этом случае окажется, что $\vec{W}^E(d)=\vec{W}^A(d)$.

На втором этапе знание E объявленных четностей пар битов и тот факт, что за счет синхронизации возникает корреляция между $\vec{W}^A(d)$ и $\vec{W}^E(d)$, позволяет ему использовать данную информацию для вычисления некоторых битов в итоговой БП.

Рассмотрим более подробно указанные уязвимости и меры их нейтрализации.

2.1. Отложенный перебор. На первом этапе метода наиболее эффективной атакой может оказаться атака «отложенный перебор», предложенная в [12]. Ее суть заключается в запоминании значений $\vec{x}(t)$, $Z^{A/B}(t)$, имеющих место при синхронизации сетей A и B, и многократном повторении синхронизаций сети E с различными начальными значениями ВК с одними и теми же сетями A и B, на входы которых подается записанный $\vec{x}(t)$, а выходы равны $Z^{A/B}(t)$. Критерием успешного окончания перебора является совпадение $S^E(d)$ с $S^A(d)$, фиксируемое по одному из критериев [10]. Очевидно, что объем перебора зависит от степени корреляции случайных величин t_{AB},t_{EB}, где $t_{AB},t_{EB}-$ количество тактов до полного совпадения ВК сетей A с B и E с A соответственно. С ростом d коэффициент корреляции изменяется от 0 при полном несовпадении ВК до 1 при полном совпадении ВК. Это свойство существенно зависит от конфигурации и параметров используемых СИНС.

В [13] показано, что для реализации процесса синхронизации, наиболее неблагоприятного для E, следует выбрать сети A и B с параметрами $k=3,n=1000,L=8$. При таком выборе параметров удается получить БП длиной $b=12000$ и достаточно серьезное отставание синхронизации сетей E и A от синхронизации A и B, т. к. имеет место $P(t_{AB}\le d)>>P(t_{AE}\le d)$. Однако более глубокий анализ показал, что сформированные

при этом компоненты векторов $\vec{W}^A(d)$ и $\vec{W}^B(d)$ не имеют равномерного распределения: значения ВК, равные L и $-L$, а также близких к ним значений, встречаются гораздо чаще, чем остальные. Это делает возможным частотный анализ $\vec{W}^A(d)$ и $\vec{W}^B(d)$.

Для успешного противостояния атаке отложенного перебора целесообразно использовать способ, предложенный в [13]. Его суть заключается в том, что при формировании совпадающих БП с помощью СИНС вместо одной синхронизации сетей A и B, производится r независимых синхронизаций с различными начальными значениями ВК, а результирующие вектора $S_r^A(d)$ и $S_r^B(d)$ вычисляются как некоторая свертка результатов каждой синхронизации:

$$S_r^A(d) = S_1^A(d) \oplus S_2^A(d) \oplus ... \oplus S_r^A(d),$$

$$S_r^B(d) = S_1^B(d) \oplus S_2^B(d) \oplus ... \oplus S_r^B(d).$$

В результате получаем бинарные последовательности длиной b, в которых каждый бит – сумма битов по модулю 2 из r слагаемых.

E осуществляя отложенный перебор, не имеет возможности сопоставлять результаты своих частных синхронизаций, с результатами частных синхронизаций сетей A и B. А поскольку при переходе к сверткам взаимная корреляция $S_r^A(d)$ с $S_r^B(d)$ с ростом r ослабляется значительно медленее, чем корреляция $S_r^E(d)$ с $S_r^A(d)$, то объем отложенного перебора существенно возрастает.

В таблице 1 приведены значения $M\left[\delta_{A,B}\right]$, $M\left[\delta_{E,A}\right]$ соответственно в числителе и знаменателе: между $S_r^A(d)$ и $S_r^B(d)$, между $S_r^E(d)$ и $S_r^A(d)$.

Таблица 1

Значения $M\left[\delta_{A,B}\right]$, $M\left[\delta_{E,A}\right]$

r	d				
	500	1000	2000	2500	3500
1	0,61/0,59	0,74/0,65	0,97/0,65	0,99/0,65	0,99/0,65
5	0,50/0,50	0,53/0,50	0,89/0,51	0,98/0,51	0,99/0,51
10	0,50/0,50	0,51/0,50	0,81/0,50	0,96/0,50	0,99/0,51

В этой таблице $\delta_{A,B} = \frac{n_{A,B}}{b}$, $\delta_{E,A} = \frac{n_{E,A}}{b}$, где $n_{A,B}, n_{E,A}$ – количество совпадающих бит в $S_r^A(d)$ и $S_r^B(d)$, $S_r^E(d)$ и $S_r^A(d)$ соответственно. Из таблицы видно, что при $r \geq 5$ величина $M\left[\delta_{A,B}\right]$ близка к 1,0 уже начиная от $d = 2500$, в то время, как величина $M\left[\delta_{E,A}\right]$остается близкой к 0,5 (0,5 свидетельствует о статистической независимости $S_r^E(d)$ и $S_r^A(d)$). В [13] показано, что увеличивая r, можно экспоненциально увеличить объем отложенного перебора (табл. 2).

Таблица 2

Объем отложенного перебора

P_{EA}	r			
	5	10	20	50
0,001	$3 \cdot 10^{15}$	$3 \cdot 10^{30}$	$3 \cdot 10^{60}$	$3 \cdot 10^{150}$
0,005	$9{,}3 \cdot 10^{12}$	$2{,}9 \cdot 10^{23}$	$2{,}8 \cdot 10^{46}$	$2{,}6 \cdot 10^{115}$
0,010	$3 \cdot 10^{10}$	$3 \cdot 10^{20}$	$3 \cdot 10^{40}$	$3 \cdot 10^{100}$
0,050	$2{,}8 \cdot 10^{7}$	$9{,}7 \cdot 10^{14}$	$2{,}8 \cdot 10^{26}$	$2{,}6 \cdot 10^{65}$

Кроме того, в [13] показано, что с ростом r закон распределения вероятностей $S_r^A(d)$ и $S_r^B(d)$, близок к равномерному, что делает неэффективным частотный анализ этих БП.

Положительным свойством комбинированного метода является и то, что на этапе синхронизации для A и B нет необходимости добиваться совпадения $S_r^A(d)$ с $S_r^B(d)$ и подтверждения этого, следовательно, и E не имеет критерия для остановки перебора.

2.2. Атака, основанная на знании четностей пар. На втором этапе метода, когда абоненты A и B оглашают четности пар БП, сформированных с помощью СИНС, у криптоаналитика E появляется возможность сравнения этих четностей с четностями своей БП и сделать определенные выводы относительно формируемого общего секрета. Оценим эффективность атаки, описанной в [1].

Для этого проведем анализ влияния параметров сетей на процесс устранения несовпадений битов на втором этапе.

Поскольку процедура устранения несовпадений битов оперирует с парами битов, то целесообразно проводить анализ на уровне пар, а не отдельных битов. Анализ может быть выполнен аналитически с использованием результатов, полученных в [1] или методом статистического моделирования.

Обозначим длину БП, сформированных путем синхронизации сетей A и B через b. Тогда число пар равно $D = \frac{b}{2}$, если b окажется нечетным, то его следует привести к четному, отбросив последний бит. Тогда согласно [1], среднее число совпадающих пар битов в анализируемых БП равно

$$m_{c,c} = \frac{b_{A,B}^2}{b^2} \cdot D = \frac{b_{A,B}^2}{2b},$$

где $b_{A,B}$ – количество совпадающих битов в БП A и B.

Среднее число пар битов, содержащих один совпадающий бит, равно

$$m_{c,н} = 2D \frac{b_{A,B}}{b} \frac{(b - b_{A,B})}{b} = \frac{b_{A,B}(b - b_{A,B})}{b}.$$

Среднее число пар битов, содержащих два несовпадающих бита, равно

$$m_{н,н} = D \frac{(b - b_{A,B})^2}{b^2} = \frac{(b - b_{A,B})^2}{2b}.$$

Пары, содержащих один совпадающий бит, в дальнейшем согласовании не участвуют, т.к. подлежат удалению. Поэтому представляет интерес только величины $m_{c,c}$ и $m_{н,н}$. В таблице 3 приведены значения этих величин в зависимости от количества совпадающих битов для $b = 12000$.

Таблица 3

Значения величины $m_{c,c}$ и $m_{н,н}$ в зависимости от количества совпадающих битов

$b_{A,B}/b$	0,500	0,583	0,666	0,750	0,833	0,9166	1,000
$m_{c,c}$	1500	2041	2666	3375	4166	5401	6000
$m_{н,н}$	1500	1041	666	375	166	41	0
$m_{c,c} + m_{н,н}$	3000	3082	3332	3750	5832	5442	6000

Обозначим БП абонентов A и B, получившиеся после прерванной синхронизации, через $S_r^A(d)$ и $S_r^B(d)$, а итоговую БП $S_r^{AB}(d)$.

После остановки синхронизации и оглашения четностей пар битов E знает, что A и B оставят для дальнейшего рассмотрения только пары, у которых четности совпадают $C_A^{(i)} = C_B^{(i)}$. Поэтому E будет рассматривать только те свои пары битов, для которых выполняется $C_E^{(i)} = C_A^{(i)} = C_B^{(i)}$. Для битов каждой из этих пар можно выдвинуть следующие гипотезы:

$$H_0 : e_j = a_j = b_j, e_{j+1} = a_{j+1} = b_{j+1};\ H_1 : e_j = \overline{a}_j = \overline{b}_j, e_{j+1} = \overline{a}_{j+1} = \overline{b}_{j+1};$$

$$H_2 : e_j = a_j = \overline{b}_j, e_{j+1} = a_{j+1} = \overline{b}_{j+1};\ H_3 : e_j = \overline{a}_j = b_j, e_{j+1} = \overline{a}_{j+1} = b_{j+1}.$$

Зная параметры сетей и d, можно априорно оценить вероятности этих гипотез путем моделирования, многократно повторяя первый этап метода и подсчитывая количество исходов в которых имело место событие, соответствующее той или иной гипотезе $P(k) \approx \frac{n(k)}{n_c}$, где $k - 0,1,2,3$; $n(k) -$ число пар, соответствующее гипотезе H_k, $n_c -$ общее число пар, у которых $C_E^{(i)} = C_A^{(i)} = C_B^{(i)}$.

В таблице 4 приведены результаты моделирования для $K = 3, n = 1000, L = 8, r = 5$.

Таблица 4

Результаты моделирования

$P(k)$	d					
	500	1000	2000	2500	3000	10000
$P(0)$	0,257	0,302	0,483	0,501	0,505	0,506
$P(1)$	0,267	0,363	0,457	0,490	0,495	0,493
$P(2)$	0,245	0,214	0,029	0,003	0,001	0,000
$P(3)$	0,245	0,215	0,029	0,003	0,001	0,000

Из всех пар битов, для которых $C_A^{(i)} = C_B^{(i)}$, в итоговую БП $S_r^{AB}(d)$ пройдут только пары, соответствующие гипотезам H_0, H_1. Поэтому E предполагает, что те биты его БП, для которых выполнялось $C_E^{(i)} = C_A^{(i)} = C_B^{(i)}$ и которые у A и B прошли в итоговую БП, с вероятностью $P(0)$ равны битам последовательностей A и B, *а с* вероятностью $P(1)$ противоположны им. Однако из табл. 2 видно, что значения вероятностей $P(0)$ и $P(1)$ в диапазоне предлагаемых значений d близки к 0,5 и, следовательно, E не может различить свои отслеживаемые биты. Данное свойство объясняется, тем корреляция БП $S_r^A(d)$, $S_r^B(d)$ и $S_r^E(d)$ очень слабая и с ростом d $S_r^E(d)$ остается практически статистически независимой от $S_r^A(d)$, $S_r^B(d)$ и, следовательно, в ней число пар, соответствующих гипотезам H_0, H_1, остается одинаковым.

Заключение. По результатам анализа и нейтрализации уязвимостей базового алгоритма формирования криптографического ключа с помощью СИНС удалось создать комбинированный метод. На первом этапе при формировании бинарной последовательности с математическим ожиданием доли несовпадающих битов менее 0,5 добавляется функция свертки, что позволяет обеспечить требуемую конфиденциальность формируемого общего секрета, а также делает данный способ устойчивым к атаке, основанной на знании четностей пар, на втором этапе. Изложенная двухэтапная процедура является, на наш взгляд, достаточно эффективным методом формирования общего секрета. В его основе лежит комбинация полученных ранее результатов. Это позволило существенно сократить количество обменов информацией и повысить криптостойкость по отношению к атаке «отложенный перебор».

Список литературы

1. Пивоваров, В. Л. Способ формирования криптографического ключа для слабо совпадающих бинарных последовательностей / В. Л. Пивоваров, В. Ф. Голиков // Информатика. – 2016. – № 3 (51). – С. 31–37.

2. Shannon, C. E. Communication theory of secrecy systems / C. E. Shannon // Bell system technical journal. – 1949. – Vol. 28, Issue 4. – P. 656–715.

3. Metzler, R. Interacting neural networks / R. Metzler, W. Kinzel, I. Kanter // Phys. Rev. E. – 2000. – Vol. 62. – №2. – P. 2555–2565.

4. Kanter, I. The Theory of Neural Networks and Cryptography, Quantum Computers and Computing / I. Kanter, W.Kinzel. − 2005. – Vol. 5, n.1. – P. 130−140.

5. Kinzel, W. Neural Cryptography / W. Kinzel, I. Kanter // 9th International Conference on Neural Information Processing, Singapore, 2002.

6. Kanter, I. Secure exchange of information by synchronization of neural networks / I. Kanter, W. Kinzel, E. Kanter//arxiv: cond/0202112v1, [cond-mat.stat-mech], 2002.

7. Kinzel, W. Interacting neural networks and cryptography / W. Kinzel, I. Kanter // Advances in Solid State Physics ; ed. B. Kramer. – Springer Verlag, 2002. – С. 122.

8. Freking, A. Learning and predicting time series by neural networks / A. Freking, W. Kinzel, I. Kanter. – 2002.

9. Плонковски, М. Криптографическое преобразование информации на основе нейросетевых технологии / М. Плонковски, П. П. Урбанович // Труды БГТУ. Сер. VI. Физико-математические науки и информатика ; под ред. И. М. Жарского. – Минск : БГТУ, 2005. – С. 161–164.

10. Ruttor, A. Dynamics of neural cryptography / A. Ruttor, I. Kanter, W. Kinzel // Phys. Rev. E, 75(5):056104, 2007.

11. Голиков, В. Ф. Формирование общего секрета с помощью искусственных нейронных сетей / В. Ф. Голиков // Системный анализ и прикладная информатика. – 2019. – № 2. – Р. 49–56.

12. Голиков, В. Ф. Атака на синхронизируемые искусственные нейронные сети, формирующие общий секрет, методом отложенного перебора / В. Ф. Голиков, А. Ю. Ксеневич // Доклады БГУИР. – 2017. – № 8.

13. Радюкевич, М. Л. Усиление секретности криптографического ключа, сформированного с помощью синхронизируемых искусственных нейронных сетей / М. Л. Радюкевич // Информатика. – № 17 (1). – С. 102–108.

УДК 519.81

КОНЦЕПТУАЛЬНО-ПРАВОВЫЕ И ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЮЗНОГО ГОСУДАРСТВА В СОВРЕМЕННЫХ УСЛОВИЯХ

А.Д. ШЕРСТНЕВ
Научно-консультативный совет Парламентского Собрания Союза Беларуси и России
г. Москва, Российская Федерация

События последних лет еще раз подтвердили реальность того, что современный мир существует в условиях информационных войн различной направленности, масштабов и интенсивности. Ведущие государства превратили свои подсистемы информационного противоборства, ранее выполнявшие обеспечивающие задачи, в самостоятельные ударные системы гибридной войны. Информационно-коммуникационные технологии и сеть «Интернет» придают информационным войнам сетецентрический характер. Отброшены все запреты и ограничения на применение информационного оружия. Даже трагическая для человечества пандемия короновируса стала информационным поводом для разрушительной мировой инфодемии.

Особенно активно информационные войны ведутся против национальных государств, таких как Беларусь и Россия, провозгласивших и осуществляющих независимый курс, защищающих свой суверенитет и национальные интересы. Объектами информационной войны являются не только государства-участники, но и Союзное государство в целом. Какой шквал информационных атак обрушился на Беларусь с середины прошлого года. Цель – «цветная революция» и государственный переворот.

Исходя из этого, Республика Беларусь и Российская Федерация обязаны иметь и развивать концептуальные документы в различных сферах своей национальной безопасности, которые являются методологической основой деятельности, в том числе в области обеспечения информационной безопасности.

В общепринятом понимании, концепция – это тот документ, который излагает комплексное видение ситуации на перспективу, определяет долговременную и текущую политику государства в данной сфере и является базой для разработки правовых основ регулирования. Считается, что доктрина является документом стратегического планирования в сфере обеспечения национальной безопасности государств, в котором развиваются положения концепций (стратегий) национальной безопасности, а также других документов стратегического планирования в указанной сфере. В отличие от концепции доктрина более полно учитывает сложившуюся ситуацию, имеет большую гибкость, конкретность и ряд других положительных моментов.

Как в прошедшие годы шло формирование и развитие концептуальных основ информационной безопасности в государствах-участниках Союзного государства?

В Российской Федерации с 2000 года реализовывалась Доктрина информационной безопасности, которая пришла на смену существовавшей тогда Концепции информационной безопасности.

В 2014–2015 годах резко и зло усилились нападки на Россию по всем возможным направлениям и поводам. Учитывая откровенно негативные изменения в условиях обеспечения национальной безопасности Российская Федерация приняла новую Стратегию национальной безопасности (Указ Президента Российской Федерации от 31 декабря 2015 года № 683).

В ответ на возросший накал информационной войны против России в 2016 году в Российской Федерации была принята новая Доктрина информационной безопасности (Указ Президента Российской Федерации от 5 декабря 2016 года № 646).

Документ создан на основе анализа угроз и оценки состояния ИБ РФ и развивает положения Стратегии национальной безопасности РФ. Документ состоит из 38 статей, разбитых на пять глав.

Текст Доктрины начинается с указания национальных интересов в сфере национальной безопасности. Далее идет перечисление основных информационных угроз в современном мире. На основании этих угроз формируются стратегические цели национальной политики, касающиеся различных сфер жизнедеятельности государства, общества и граждан.

К национальным интересам отнесено «обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации» и «продвижение достоверной информации о госполитике России и ее официальной позиции по социально значимым событиям в стране и мире». При этом должны обеспечиваться конституционные права и свободы, достойное качество и уровень жизни граждан, суверенитет и территориальная целостность РФ, ее устойчивое социально-экономическое развитие, а также государственная безопасность.

Среди основных информационных угроз выделены, такие как «специальные службы используют методы информационно-психологического воздействия на граждан, внешнее информационное воздействие размывает традиционные российские духовно-нравственные ценности (особенно у молодежи)», «террористические и экстремистские группировки нагнетают межнациональную и социальную напряженность, занимаются пропагандой, привлекают новых сторонников», «растет число преступлений, связанных с нарушением конституционных прав и свобод человека, неприкосновенности частной жизни, защиты персональных данных. Эти преступления становятся все изощреннее», «управление Интернетом на принципах справедливости и доверия между разными странами невозможно».

В Доктрине стратегическими целями определены «нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества», «противодействие использованию информационных технологий для пропаганды экстремизма, ксенофобии и национализма», «нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей». Особо подчеркнута стратегическая цель – «формирование у граждан культуры личной информационной безопасности».

Два года назад произошло несомненно значимое событие в развитии концептуальных основ обеспечения информационной безопасности Республики Беларусь, а также Союзного государства в целом. Постановлением Совета безопасности Республики Беларусь от 18 марта 2019 года № 1 утверждена Концепция информационной безопасности Республики Беларусь.

Авторы постарались включить все прогрессивные наработки в области ИБ. Поэтому документ получился объемным (105 статей в 27 главах 7 разделов).

Авторы подчеркивают, что белорусская Концепция информационной безопасности является абсолютно самостоятельной национальной разработкой, учитывающей белорусские особенности и подходы. Кроме этого, ряд тезисов и конструкций Концепции являются оригинальными и новыми. Концепция содержательно объединяет в себе европейский и евразийский подходы, сводя воедино и без ущерба логике информационную безопасность и кибербезопасность. В концепции реализуется подход, при котором безопасность рассматривается не как абсолютная категория, а как конкретная защищенность от выделенных угроз.

Беларусь, как и все страны, не может игнорировать принципиально новые риски, связанные с информатизацией, так как нарастание в мире конфликтности и отсутствие в информационной сфере четких правил поведения превращают эти риски в реальные угрозы конституционным основам и всестороннему развитию любого государства.

При рассмотрении проекта Концепции на заседании Совета безопасности РБ в 2019 году А.Г. Лукашенко, что «вызывает беспокойство наращивание деструктивных воздействий на общество, манипулирование массовым сознанием, распространение недостоверной информации. Именно с них начинаются социальные катаклизмы современности. В результате страдают миллионы людей, меняется политическая карта мира. Отодвигаются на второй план общепринятые нормы морали и нравственности. Жизнедеятельность любого государства становится все более уязвимой от компьютерных инцидентов». Беларусь не ограждена от кибератак и киберпреступности. Впервые в публичном документе указывается готовность государства непрерывно выявлять риски, вызовы и угрозы в информационной сфере и реагировать на них. Помимо эффективной работы СМИ в Концепции подчеркивается важ-

ность активного присутствия государства в Интернете: речь идет не только об официальных сайтах государственных органов, но и о блогосфере, мессенджерах и социальных сетях.

В числе обозначенных практических мер и аспектов, связанных с обеспечением информационной безопасности, считается необходимым более внимательно подходить к защите главных конституционных основ общества, прежде всего связанных с государственным суверенитетом. Вместе с тем, государство, безусловно, заинтересовано и в том, чтобы люди получали максимально полную и достоверную информацию. Имели возможность защитить свои личные права в медиапространстве и в целом повышали комфортность жизни за счет новейших достижений»

В разделе 4 Концепции заявлено, что «информационная политика Республики Беларусь нацеливается на продвижение таких жизненных приоритетов, как гуманизм, миролюбие, добрососедство, справедливость, взаимопомощь, крепкие семейные отношения, здоровый образ жизни, созидательный труд, принятые в белорусском обществе нормы морали и нравственности, позитивное правосознание».

В Беларуси нужно расширить сферу влияния отечественных средств массовой информации. Главное – быстро, четко, максимально полно доносить до людей правдивую информацию. необходимо предпринимать меры по повышению объема, разнообразия и качества национального вещания, доверия населения к официальным массмедиа. Требуется системный контроль за распространением незаконной информации.

Общее впечатление состоит в том, что Концепция отражает государственную позицию по всем аспектам информационной сферы. Можно только добавить некоторые моменты.

Провозглашение, достижение и обеспечение информационного суверенитета страны предопределяет необходимость противодействия еще одной актуальной угрозе, которая исходит из сети Интернет, но недостаточно артикулирована в Концепции. Провокационный контент, фейковые вбросы и иные негативные материалы пропагандистского характера, отрицательно воздействуют на индивидуальное и групповое социально-психологическое состояние населения, что обесценивает усилия государства по обеспечению информационного суверенитета. В этих условиях управление национальным сегментом сети Интернет предполагает непрерывный (24/7) мониторинг контента и обязательный контрпропагандистский ответ. Основным способом борьбы видят наполнение ответственным контентом информационного пространства, чтобы люди могли ориентироваться на тех людей и на те новостные источники, которым они доверяют. Надо распространять некие практики, стандарты ответственного поведения в информационной сфере. Надо думать, и об ответственности за злонамеренные действия в этой сфере.

В качестве итога анализа концептуальных документов необходимо отметить, что к настоящему моменту Беларусь и Россия сформировали достаточную концептуальную основу для законодательного обеспечения своей информационной безопасности.

Федеральный закон 149-ФЗ «Об информации, информационных технологиях и защите информации», принятый в 2006 году, является базовым в правовом регулировании информационных отношений.

Преимуществом данного закона является подробная детализация и конкретизация норм закона именно в федеральном законе, что позволяет каждому участнику информационных отношений получить прямой правовой ответ по вопросам его обязанностей, прав и ответственности. В связи с этим снижается потребность в дополнительных подзаконных актах и нормативных правовых документах. Правда это обязывает законодателей активно и своевременно вносить в закон изменения и дополнения с учетом возникающих проблемных ситуаций в информационной сфере и правоприменительной практике. За 15 лет после ввода закона в действие приняты 44 изменяющих документа, последний в марте текущего года.

Основной закон в сфере информационной безопасности Республики Беларусь «Об информации, информатизации и защите информации».

Данный закон отличается от федерального закона Российской Федерации большей общностью положений, что предопределяет необходимость его «расшифровки» через комплекс других нормативных правовых документов. Закон по-иному структурирован (в нем имеются главы, которых нет в российском законе).

Важное значение во взаимодействии государств-участников Союзного государства в информационной сфере имеет заключенное в 2013 году «Соглашение между Правительством Республики Беларусь и Правительством Российской Федерации о сотрудничестве в области обеспечения международной информационной безопасности».

Актуальной задачей Беларуси, России и Союзного государства в целом является дальнейшее совершенствование (гармонизация, унификация) законодательств государств-участников и формирование нормативно-правовой базы Союзного государства в информационной сфере.

Таким образом, проведенный анализ показывает, что принятые к настоящему времени концептуальные, законодательные и договорно-правовые акты Беларуси и России в основном соответствуют потребностям наших стран по защите своих жизненно важных интересов в информационной сфере и укреплению их информационной безопасности, по обеспечению общей безопасности Союзного государства.

Анализ подтверждает, на мой взгляд, современный тренд, который становится приоритетным при разработке новых доктринальных и законодательных документов в сфере информационной безопасности. Речь идет о расширении и углублении гуманитарных основ информационной безопасности. Документы приобретают, как в свое время говорили, все большее «человеческое измерение». Правда это не очень касается языка изложения и масштабов распространения этих знаний среди многомиллионной аудитории.

Человек в конечном итоге является и объектом, и субъектом информационных отношений. Применительно к человеку среди принципов правового регулирования отношений в сфере информации, информационных технологий и защиты информации в соответствии с федеральным законом выделим следующие:

- свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- достоверность информации и своевременность ее предоставления;
- неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия.

В 60–70-е гг. прошлого века, разрабатывая сеть Arpnet для военного командования, США не предполагали создать Интернет как всемирную сеть и базу знаний. В конце 20 – начале 21 века бурное развитие систем и средств мобильной связи, расширение зон Wi-Fi сделало Интернет доступным для каждого владельца смартфона в режиме 24/7. А в итоге этих процессов появилось информационное оружие, позволяющее манипулировать сознанием и поведением миллионов людей. В Союзном государстве примерно 98–100 миллионов пользователей Интернета.

По оценке одного из экспертов, Интернет является не только всемирной базой знаний и всемирной сетью общения, но и всемирной информационной помойкой. Наличие в стране миллионов частных электронных средств, имеющих доступ к Интернету, представляет своего рода гигантский пылесос, бесконтрольно и ежеминутно втягивающий из него зловредный информационный мусор.

Из-за ситуации с коронавирусом значительная часть человеческой деятельности перешла в онлайн, а сеть «Интернет» породила огромные потоки информации, совладать с которыми многим не под силу. Коронавирус стал поводом для большого количества фейков, которые не только пагубно влияют на психическое состояние и здоровье человека.

Инфодемия на почве коронавируса, которая распространяется еще быстрее, чем сама инфекция, по мнению экспертов, препятствует борьбе с COVID-19. (Термин «инфодемия» Всемирная организация здравоохранения (ВОЗ) начала использовать в феврале 2020 года. Так назвали не соответствующие действительности тексты, которые сопровождают пандемию. На сайте ВОЗ даже появился целый раздел, посвященный таким материалам).

«В ситуации, когда интернет и СМИ являются практически единственным источником информации и по сути шансом для обретения хоть какой-то определенности в настоящем и будущем, человеку свойственно поддаваться панике и цепляться за каждую

информацию, которая придает ему определенности и понимания, что происходит и что будет дальше», – так считает главный медицинский психолог Минздрава России, декан факультета психологии МГУ имени М. В. Ломоносова Юрий Зинченко.

Источники поддержки у нас у всех разные. Кому-то достаточно ощутить поддержку близких, чтобы стабилизировать свое психологическое состояние, кому-то нужна профессиональная помощь психологов. А кому-то необходимо постоянно иметь доступ к актуальной информации о ситуации в стране и мире. Здесь проблема в том, что наравне с объективными фактами Сеть заполнена фейковыми и неподтвержденными сообщениями. К такому общество готово не было: отличать факты от лжи в Сети умеют далеко не все. При этом фейки, по словам психолога, напрямую влияют на состояние человека. «Неадекватная и необъективная информация может повышать уровень нашего стресса, тревоги и даже привести к депрессии», – заявил Зинченко.

Кроме того, «альтернативная информация зачастую меняет модель поведения, так как фейки вызывают недоверие к властям. На памяти у нас ситуация, когда в Британии сожгли 20 5G-вышек потому что в интернете пустили слух, что через эти волны уничтожается иммунитет. Как, не уточнили, но вот так горело примерно в пяти городах, может и больше.

В борьбе с «сетевой» проблемой участвовать может каждый. И начинать нужно с азов – научиться работать с информацией. В первую очередь, необходимо распознавать вредную и недостоверную информацию. Людям следует научиться распознавать фейки и нагнетания в Сети и отличать их от объективной и достоверной информации. Чаще всего фейковые новости отличаются чрезмерной эмоциональностью, но при этом и малоинформативностью. Обычно кибермошенники ориентируются на наши негативные чувства, вызывают быстрые реакции за счет громких, но ничем и никем не подтвержденных заявлений.

Если понимание реальной обстановки в мире помогает человеку успокоиться, за информацией необходимо обращаться только к достоверным источникам и официальным порталам. При этом лучше всего отследить, в какое время на проверенных официальных источниках появляется актуальная информация, и встроить просмотр этого источника в свой жизненный график.

Мы хотим сейчас всегда быть в курсе актуальной информации, но от того, что мы будем постоянно искать новую информацию, ничего не изменится. Может, это даже и усугубит наше состояние. При этом в самом чтении новостей ничего плохого нет, если знать меру. Понимание реальной обстановки может успокоить.

При этом жить в «сетевом» вакууме не получится: различные лженовости так или иначе будут попадаться на глаза. Поэтому главное средство в борьбе с последствиями фейковой информации – умение человека справляться со стрессом, тревогой и другими негативными эмоциями и смотреть на мир объективно. Если мы примем условия, в которых мы временно оказались, мы сможем освободиться от навязчивых мыслей.Для того чтобы негативные реакции не смогли нас заблокировать и увести в деструктивное поведение, нам надо всего лишь поставить перед собой адекватные и конструктивные цели в данный период, продумать четкий график жизни, который будет для нас признаком стабильности и понятности.

Проблематика фейковых новостей, которые поднимали уже не один год, обострилась донельзя – люди, напуганные «новостями», сидят в ожидании чуть ли не апокалипсиса. В погоне за просмотрами, лайками порой происходит нечто невообразимое.

Размышляют: разрешено ли военным стрелять? Для чего толпы омоновцев на улицах? Чем грозит чрезвычайное положение? Подобные размышления это и есть нагнетание и паника. Все это, конечно, как правило, мягко говоря, преувеличение и бизнес – ничего личного.

Наша клиповость мышления – такое уж время скоростное – падкое на яркие фразы и заголовки. Но, к сожалению, не на суть. Будем мониторить дальше и верить по классике, что разум победит.

Понятно, что дезинформация не является смертельным оружием сама по себе – фейк непосредственно не может убить человека. Но получение вместо правдивой информации фейковой способно ухудшить шансы человечества в целом и отдельно взятого человека на преодоление существующей угрозы.

Усилия, направленные на то, чтобы остановить людей, которые делятся ложными новостями, дезинформацией и вредными советами в социальных медиа, могут снизить уровень социальной напряженности. Должен быть активизирован общественный контроль за распространением в информационном пространстве незаконной и недостоверной информации. Необходимо развивать сеть фактчекеров, которые активно проверяют информацию и сигнализируют соответствующей администрации для принятия мер. Впрочем, опасность представляют не только собственно фейки, но и попытка медиа и пользователей социальных сетей нагнетать панику и истерику, искажая и додумывая достоверную информацию.

Очевидно, что, если люди не верят официальным источникам информации, любые заявления, направленные на сдерживание паники, лишь способны ее распространить. По мнению британских ученых, люди быстрее делятся неправдивыми историями, чем достоверной онлайн-информацией и более склонны верить в теории заговора в случае недоверия к органам власти. Таким образом, если власть страны не имеет авторитета, шансы на неадекватное реагирование общества на проблемную ситуацию увеличиваются, и, наоборот, если власти доверяют, к ее аргументам будут прислушиваться и выполнять ее рекомендации.

В информационном обществе, к которому идут наши страны, конституционное право гражданина на его информационную безопасность предопределяет как обязанность человека лично участвовать в работе по ее обеспечению, так и личную ответственность за собственную ИБ. Эта позиция должна пропагандироваться (а лучше – внушаться) с детского возраста. Надежда на то, что родители обучат своих детей безопасному пользованию Интернетом и воспитают у них критическое отношение к циркулирующей в нем информации, не оправдана потому, что большинство людей в возрасте до 50 лет само интернет-зависимо и зачастую подает лишь негативный личный пример. Необходимо искать новые, может и нетрадиционные, пути, методы и средства внедрения такой позиции в индивидуальное и массовое сознание.

Настала пора очень серьезно заняться просвещением населения по вопросам повседневной информационной безопасности. Необходима разработка учебных, методических программ и материалов практической направленности, которые предстоит максимально широко и настойчиво внедрять в сознание пользователей по всем возможным каналам всеми доступными способами. Эта работа будет более эффективна в рамках государственно-частного партнерства.

Что касается информационного нейтралитета (кстати этому понятию не дано определения), то он может быть только вовне страны. Нейтральное отношение к процессам и событиям в информационной сфере государства, вседозволенность в формировании и распространении информации, всеядность в ее потреблении дезориентируют и разлагают общество, подрывают основы государственности. Государства Европы пожинают горькие плоды толерантности в своих информационных пространствах. На наш взгляд, такой подход к информационному нейтралитету должен жестко проводиться в дальнейшей разработке теории ИБ, практической работе по ее реализации.

В Концепции ИБ РБ записано, что «не допускается распространение информации, направленной на пропаганду войны, экстремистской деятельности или содержащей призывы к такой деятельности, потребления наркотических средств и им подобных веществ, порнографии, насилия и жестокости, иной информации, запрещенной законодательством. На государственном уровне реализуются меры по воспрепятствованию распространению информации, способной нанести вред национальным интересам, и недостоверных сведений, а также по снижению анонимности в информационном пространстве. При трансляции контента не разрешается применение скрытых технологических приемов, воздействующих на подсознание людей или оказывающих вредное влияние на их здоровье».

Активное противодействие негативному информационно-психологическому воздействию – насущная задача сейчас и на перспективу, так как, по оценке президента Республики Беларусь А.Г. Лукашенко: «Информационными потоками размывается национальный менталитет, самобытность стран и народов. Существенно меняются социальные связи человека, стиль мышления, способы общения, восприятие действительности. Всему этому следует противопоставить принципы гуманизма и справедливости, приоритеты крепких семейных отношений и здорового образа жизни».

РЕЗОЛЮЦИЯ XXVI НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ «КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ»

С 25 по 27 мая 2021 года в г. Минске состоялось ежегодное мероприятие Союзного государства – XXVI научно-практическая конференция «Комплексная защита информации» (далее – конференция).

Организаторы конференции:

Постоянный Комитет Союзного государства;

Парламентское Собрание Союза Беларуси и России;

Аппарат Совета Безопасности Российской Федерации.

Проведение конференция осуществлялось государственным предприятием «НИИ ТЗИ» (Беларусь) при поддержке Медиа Группы «Авангард» (Россия).

В работе конференции приняли участие 183 представителя Беларуси и России. Среди участников конференции 16 докторов наук, 26 кандидатов наук, среди них 14 профессоров, 17 доцентов, а также специалисты-практики, руководители государственных и коммерческих организаций, специализирующиеся на решении практических вопросов в сфере обеспечения информационной безопасности.

На конференции рассмотрены актуальные вопросы обеспечения информационной безопасности в Союзном государстве.

Целью настоящей конференции стало рассмотрение и обсуждение тем:

перспективные направления технической защиты информации;

криптография для граждан и государства;

специалист по информационной безопасности – профессия будущего;

вопросы стандартизации в области информационной безопасности;

кибербезопасность и информационное противоборство;

перспективные технологии информационной безопасности.

Особое место на конференции было отведено обмену опытом по вопросам информационного противоборства в современных реалиях.

Конференция считает, что между ее участниками состоялся плодотворный обмен опытом в области исследований, разработки и внедрения теоретических, методологических, нормативных, организационно-технических, правовых и гуманитарных вопросов обеспечения информационной безопасности.

Конференция отмечает значение и актуальность для государств-участников Союзного государства следующих задач и направлений деятельности:

выработка совместных подходов по обеспечению безопасности государственных информационных ресурсов Союзного государства с учетом современных угроз безопасности информации;

формирование единых рекомендаций по использованию сертифицированных средств защиты информации, разработанных в рамках Союзного государства, для нейтрализации известных уязвимостей, особенно для критически важных систем информационной безопасности;

активизация сотрудничества по обмену сведениями об угрозах безопасности информации и уязвимостях в информационных системах Беларуси и России;

реализация возможности обмена специалистами с целью прохождения повышения квалификации в области информационной безопасности за счет бюджета Союзного государства, в том числе по программе академической мобильности;

гармонизация образовательных стандартов в области информационной безопасности России и Беларуси (программы двух дипломов);

выработка совместных подходов к разработке государственных образовательных стандартов высшего образования по новому направлению подготовки специалистов «Информационная безопасность социотехнических систем»;

организация совместных студенческих чемпионатов по проведению киберучений по выявлению и пресечению компьютерных атак на КИИ Союзного государства и повышению профессионального мастерства.

Кроме того, положительно оценивается практика проведения в рамках конференции «Школы молодых ученых». Отдельно отмечается растущий вклад молодых ученых и специалистов в научную деятельность в сфере защиты общих информационных ресурсов Союзного государства.

Участники конференции постановили:

1. Одобрить работу Оргкомитета и результаты XXVI научно-практической конференции «Комплексная защита информации».

2. Федеральным органам исполнительной власти Российской Федерации и республиканским органам государственного управления Республики Беларусь проработать вопрос заключения международного договора, устанавливающего нормы, определяющие порядок признания электронных цифровых подписей (электронных подписей), созданных в другом государстве, в целях обеспечения обмена юридически значимыми электронными документами.

3. Рекомендовать организаторам провести XXVII научно-практическую конференцию «Комплексная защита информации» в 2022 году в г. Светлогорске Калининградской области (Российская Федерация).

4. Государственному предприятию «НИИ ТЗИ» организовать публикацию материалов конференции в третьем квартале 2021 года.

Принята на пленарном заседании
27 мая 2021 года, г. Минск

СОДЕРЖАНИЕ

КРИПТОГРАФИЯ ДЛЯ ГРАЖДАН И ГОСУДАРСТВА

СПЕЦИАЛИСТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – ПРОФЕССИЯ БУДУЩЕГО

ВОПРОСЫ СТАНДАРТИЗАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КИБЕРБЕЗОПАСНОСТЬ И ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО

ПЕРСПЕКТИВНЫЕ ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ШКОЛА МОЛОДЫХ УЧЕНЫХ

ЗАОЧНЫЕ ДОКЛАДЫ

Научное издание

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXVI научно-практической конференции

Ответственный за выпуск *С. Н. Касанин*
Компьютерная верстка, корректура *И. В. Коновалов*

Подписано в печать 22.07.2021.
Формат 60x84/8. Бумага офсетная. Печать цифровая.
Усл. печ. л. 43,17. Уч.-изд. л. 28,52.
Тираж 60 экз. Заказ 416.

Издатель:
Индивидуальный предприниматель Сивчиков Владимир Николаевич
Свидетельство о государственной регистрации издателя, производителя,
распространителя печатных изданий от 24.04.2014 за № 1/325.
Пр. Независимости, 72-12, 220012, г. Минск.
siuchykau@gmail.com

Полиграфическое исполнение:
Общество с ограниченной ответственностью «Тупринт»
Свидетельство о государственной регистрации № 191790459 от 12.09.2012.
Ул. Первомайская, 24, к.2, пом. 109, 220088, г. Минск.