



КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

МАТЕРИАЛЫ
XXVIII НАУЧНО-ПРАКТИЧЕСКОЙ
КОНФЕРЕНЦИИ



23-25 мая 2023 года



КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXVIII научно-практической конференции

Гомель, 25–27 мая 2023 г.

Минск,
2023

УДК 004((470+571)+476)
ББК 32.81(4Бен+2)
К63

Ответственный за выпуск:

Д.Н. Арестович, заместитель директора по научной работе
государственного предприятия «НИИ ТЗИ», канд. техн. наук

К63

Комплексная защита информации: материалы XXVIII
науч.-практ. конф., Гомель, 23–25 мая 2023 г. – Минск : УГЗ МЧС
Республики Беларусь, 2023. – 277 с.
ISBN 978-985-590-203-5

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

Адресуются исследователям, практическим работникам и широкому
кругу читателей.

Тезисы не рецензировались, ответственность за содержание несут авторы.

УДК 004((470+571)+476)
ББК 32.81(4Бен+2)

ISBN 978-985-590-203-5

© Государственное учреждение образования
«Университет гражданской защиты МЧС
Республики Беларусь», 2023

ОРГКОМИТЕТ КОНФЕРЕНЦИИ

СОПРЕДСЕДАТЕЛИ

БЕЛОКОНЕВ Олег Алексеевич, Председатель комиссии Парламентского собрания Союза Беларуси и России по безопасности и обороне, Председатель Постоянной комиссии Палаты представителей Национального собрания Республики Беларусь по национальной безопасности

ХРАМОВ Олег Владимирович, заместитель Секретаря Совета Безопасности Российской Федерации

ЧЛЕНЫ ОРГКОМИТЕТА

КУБРИН Алексей Александрович, заместитель Государственного секретаря – член Постоянного Комитета Союзного государства

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

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

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

КОВАЛЕНКО Андрей Петрович, Вице-президент Академии криптографии Российской Федерации, доктор технических наук, профессор

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

ХАРИН Юрий Семенович, директор НИИ прикладных проблем математики и информатики БГУ, доктор физико-математических наук, академик НАН Беларуси

СМИРНОВ Алексей Владимирович, Министерство обороны Республики Беларусь

ЯЗОВ Юрий Константинович, главный научный сотрудник ФАУ «ГНИИИ ПТЗИ ФСТЭК России», доктор технических наук, профессор

СИЛИЦКИЙ Андрей Геннадьевич, Комитет государственной безопасности Республики Беларусь

КОЗЛОВСКИЙ Игорь Анатольевич, заместитель начальника Белорусской железной дороги

ПРОГРАММНЫЙ КОМИТЕТ

СОПРЕДСЕДАТЕЛИ

КОВАЛЕНКО Андрей Петрович, Вице-президент Академии криптографии Российской Федерации, доктор технических наук, профессор

ХАРИН Юрий Семенович, директор НИИ прикладных проблем математики и информатики БГУ, доктор физико-математических наук, академик НАН Беларуси

СЕКРЕТАРИ

АРЕСТОВИЧ Дмитрий Николаевич, заместитель директора по научной работе государственного предприятия «НИИ ТЗИ», кандидат технических наук, Республика Беларусь

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

ЧЛЕНЫ ПРОГРАММНОГО КОМИТЕТА

БОБОВ Михаил Никитич, профессор БГУИР, 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, ФБК CyberSecurity, Советник по вопросам ИБ, кандидат технических наук

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

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

МЕЛЬНИКОВ Сергей Юрьевич, доцент кафедры прикладной информатики и теории вероятностей, ФГАОУ ВО «Российский университет дружбы народов», доктор физико-математических наук

МЕЩЕРЯКОВ Роман Валерьевич, главный научный сотрудник ИПУ РАН, доктор технических наук, профессор, Российская Федерация

ФИЛИППОВИЧ Андрей Геннадьевич, Оперативно-аналитический центр при Президенте Республики Беларусь

Выступление
Председателя комиссии Парламентского собрания Союза Беларуси и России
по безопасности и обороне
Белоконева Олега Александровича

Уважаемые организаторы, участники и гости конференции!

От имени депутатов Парламентского Собрания и от себя лично приветствую вас на открытии двадцать восьмой научно-практической конференции «Комплексная защита информации». Это значимое ежегодное событие для специалистов и ученых в области защиты информации. Важное значение нынешнего мероприятия обусловлено тем, что глобальные исторические процессы вновь вывели мировые центры силы к цивилизационному противостоянию. Коллективный Запад развернул войну во всех сферах, в том числе экономической, политической и информационной.

В своем стремлении уничтожить Российскую Федерацию как государство и как единый целостный субъект мировой политики Западом ведется кампания по навязыванию России и ее союзникам чуждых ценностей, морали и поведенческих установок, неестественных подходов к семье и воспитанию детей. В тоже время в западном информационном пространстве блокируются любые попытки продвижения идей и ценностей Русского мира. Дошло до того, что ряд западных политиков публично призывают к уничтожению всей русской цивилизации и русской нации, чего себе не позволяли немецкие захватчики в ходе Великой Отечественной войны.

Не менее мощное давление оказывается и на союзную России Беларусь, поскольку россияне и белорусы являются братскими народами с едиными ценностями, целями, пониманием справедливости и счастья. Поэтому Западом предпринимается максимум усилий, чтобы разрушить это единство и при первой же возможности сменить в республике власть на русофобскую и более управляемую извне, что доказали недавние события. В СМИ разжигается костер ненависти, трубящий о «российской угрозе».

Вышеизложенное показало, что информационное пространство в силу активного развития информационно-телекоммуникационных технологий стремительно меняется, формируя новые, все более сложные угрозы. При этом существующая система обеспечения информационной безопасности государства не всегда успевает учитывать указанные современные тенденции, что ставит вопросы по дальнейшему ее совершенствованию. И как показали события последних месяцев, в том числе в силу образовавшегося ценностного вакуума, скорейшей проработки и уточнения требуют вопросы, связанные с целями развития государства и общества.

Учитывая союзнические отношения, общие культурное и историческое прошлое, единые ценностные ориентиры, позволяющие противостоять коллективному Западу, актуализация так называемых идеологических концепций требует совместной работы в рамках Союзного государства. Это упростит построение эффективной системы обеспечения информационной безопасности наших государств и позволит в быстро меняющемся мире сохранить свою субъектность, вектор национального развития и способность самостоятельно определять свой путь.

В современных геополитических условиях безопасность информационного пространства Союзного государства отвечает жизненно важным интересам Беларуси и России, а сотрудничество двух стран в информационной сфере является одним из важных направлений обеспечения безопасности Союзного государства, позволяет эффективно противодействовать деструктивному влиянию недружественных государств. Защищая безопасность граждан в Союзном государстве, мы будем действовать адекватно вызовам и угрозам. Российская Федерация и Республика Беларусь ответственно подходят к совершенствованию механизмов на этом актуальном направлении сотрудничества. Для наших стран жизненно важно совместное противодействие угрозам в информационной сфере.

Депутаты Парламентского Собрания Союза Беларуси и России уделяют серьезное внимание вопросам информационной безопасности. При их участии разработана Концепция информационной безопасности Союзного государства, которая утверждена 22 февраля 2023 г. постановлением Высшего Государственного Совета Союзного Государства.

Документ является итогом тесного взаимодействия аппаратов советов безопасности, внешнеполитических ведомств и иных компетентных органов двух стран в сфере совместного противодействия современным информационным вызовам и угрозам на основе прочного правового фундамента.

Подводя итог, необходимо подчеркнуть, что защита информации от современных вызовов и угроз является одной из основных задач в деле обеспечения национальной безопасности государств-участников и общей безопасности Союзного государства, для выполнения которой необходим ответственный подход к решению задач в сфере информационной безопасности, совершенствование механизмов противодействия возникающим угрозам, проведение совместных практических мероприятий, направленных на укрепление информационной безопасности и противодействие противоправной деятельности в информационном пространстве.

Уважаемые друзья!

Убежден, что озвученные в ходе конференции мнения и выработанные по ее итогам рекомендации будут служить целям дальнейшего сближения наших государств на благо наших народов.

Желаю всем участникам конференции плодотворной работы!

**ПОСТОЯННЫЙ КОМИТЕТ
СОЮЗНОГО ГОСУДАРСТВА**

119034, г. Москва, Еропкинский пер., д. 5, стр. 1
тел./факс: (495) 986-27-44, e-mail: mail@postkomsg.com

23 мая 2023, № 8/1

На № _____ от _____

Участникам
научно-практической конференции
«Комплексная защита информации»

Уважаемые участники конференции!

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

Обеспечение информационной безопасности государства и общества во всех видах его деятельности – важная тема научных исследований, как в России, так и в Беларуси.

Сегодня перед нами стоит задача проанализировать проблемные вопросы в области защиты и обеспечения информационной безопасности, обсудить предложения по их решению. Широкая тематика сегодняшних докладов свидетельствует о том, что эта тема не изолированный вопрос одного ведомства, одного государства, а неотъемлемая составляющая безопасности Союзного государства.

Критерии, стандарты и правила в области защиты информации необходимо вырабатывать общими усилиями в ходе таких мероприятий, как сегодняшняя конференция. Только таким образом нам удастся достичь максимального эффекта.

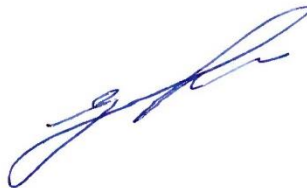
Важно отметить, что в феврале 2023 года Высший Государственный Совет Союзного государства утвердил Концепцию информационной безопасности Союзного государства, основа которой была заложена «на полях» нашего ежегодного мероприятия.

Концепция определяет основы для формирования согласованной государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также выработки мер по совершенствованию систем обеспечения информационной безопасности государств-участников Договора о создании Союзного государства.

Накопленный за это время уникальный опыт сотрудничества российских и белорусских специалистов и ученых нашел свое воплощение в успешной реализации четырех совместных программ в области информационной безопасности и разработке новой программы Союзного государства для выполнения этих задач в новых условиях.

Полагаю, что конференция станет вкладом в развитие масштабного российско-белорусского диалога, поможет определить приоритетные направления сотрудничества.

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



А.Кубрин

Приветственное слово начальника Оперативно-аналитического центра при Президенте Республики Беларусь

От имени Оперативно-аналитического центра при Президенте Республики Беларусь и от себя лично приветствую участников XXVIII научно-практической конференции «Комплексная защита информации»!

Согласованные действия Республики Беларусь и Российской Федерации в области внешней политики, экономики, обороны, дальнейшие шаги по объединению в рамках Союзного государства вызывают противодействие со стороны США и их союзников, стремящихся сохранить свое доминирование в мировых процессах. Реализуемая недружественными странами политика предусматривает политическое, экономическое, военное и информационное давление на наши страны.

В таких условиях развитие информационных ресурсов, расширение областей их применения, являющихся значимыми факторами социально-экономического развития Российской Федерации и Республики Беларусь, сопровождаются усилением угроз информационной безопасности Союзного государства.

В связи с этим проблема совершенствования научно-технического обеспечения защиты информации в информационных системах Союзного государства и государств-участников, обеспечения безопасности критически важных объектов информатизации Республики Беларусь и объектов критической информационной инфраструктуры Российской Федерации, а также при их взаимодействии и совместном использовании является актуальной и перспективной.

Настоящая конференция является мероприятием Союзного государства, представляет собой возможность для обсуждения наиболее значимых проблем по совершенствованию организационных, правовых и технических мер в области защиты информации и позволит обменяться опытом по актуальным вопросам информационной безопасности Республики Беларусь и Российской Федерации.

Желаю всем участникам конференции успехов, плодотворной работы, налаживания взаимовыгодных профессиональных взаимоотношений, а также принятия выверенных и эффективных решений в сфере обеспечения информационной безопасности Союзного государства!

*Начальник
Оперативно-аналитического центра
при Президенте Республики Беларусь*

А.Ю.Павлюченко

**Приветствие от Федеральной службы по техническому
и экспортному контролю
(заместитель начальника управления ФСТЭК России С.В. Бондаренко)**

Уважаемые Олег Алексеевич и Олег Владимирович!
Уважаемые участники и организаторы 28-й 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. Объемы глобального рынка информационных услуг и технологий ежегодно стремительно растут.

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 актуальной становится задача предотвращения использования информационных технологий для решения задач, противоречащих интересам обеспечения мира и стабильности, суверенитета и безопасности государств, безопасности граждан.

Продолжается наращивание и совершенствование средств разведки, методов и способов добывания информации, а также воздействия на нее.

Очевидно, что в условиях масштабного нарастания актуальности угроз информационной безопасности и реализации недружественными странами санкционной политики поиск эффективных путей решения актуальных задач защиты информации в государственных информационных системах, в системах обеспечения безопасности персональных данных и значимых объектов критической инфраструктуры, 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, по нашему мнению, 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 не только будут 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.

**НАЦИОНАЛЬНАЯ
АКАДЕМИЯ НАУК
БЕЛАРУСИ**



**НАЦЫЯНАЛЬНАЯ
АКАДЭМІЯ НАВУК
БЕЛАРУСІ**

ПРИВЕТСТВИЕ
Председателя Президиума
Национальной академии наук Беларуси
академика Гусакова Владимира Григорьевича

Уважаемые участники и гости конференции!

От имени Национальной академии наук Беларуси и от себя лично приветствую вас на XXVIII научно-практической конференции «Комплексная защита информации».

Сегодня перед мировым сообществом встает множество проблем, которые невозможно решить, пользуясь ресурсами и руководствуясь интересами только одного государства. Координация усилий различных государств и их интеграция – единственный выверенный путь поиска ответов на глобальные вызовы современности, будь то устойчивое развитие геополитической системы на принципах многополярности, террористическая угроза, социально-экономический, экологический, продовольственный кризисы. Все эти проблемы в большей или меньшей степени касаются и наших стран.

Беларусь и Россия, геополитические партнеры и исторические соседи, веками жили рядом, взаимодействовали и сотрудничали. Бесспорно, механизмы этого сотрудничества следует укреплять и развивать. Иного не дано.

Тесное взаимодействие российского и белорусского государств является архиактуальной задачей, решение которой напрямую способствует укреплению национальной и экономической безопасности, а также сохранению ценностных основ наших народов.

В условиях беспрецедентного санкционного давления накопленный уникальный опыт в сфере информационной безопасности белорусских и российских ученых должен найти свое воплощение в реализации совместных программ и мероприятий Союзного государства.

Сегодняшнее научное мероприятие собрало многих исследователей из разных областей сферы информационной безопасности, и хочется думать, что благодаря плодотворной коммуникации каждый участник конференции получит ответы на интересующие вопросы.

Конференция – это всегда обмен знаниями, а знания позволяют решать задачи, которые волнуют общество.

Желаю всем участникам конференции новых достижений, идей и методов их решений, творческих успехов, благополучия и крепкого здоровья.

Уважаемые участники конференции!

Информационная безопасность – одно из ключевых направлений развития информационных технологий в Республике Беларусь и Российской Федерации в 2022 году и останется таким в перспективе.

Кибератаки на информационную инфраструктуру предприятий и государственных организаций, утечка персональных данных, информационное противоборство в сети Интернет, отказ зарубежных производителей в технической поддержке оборудования и программного обеспечения на территории Союзного государства – это те вызовы и угрозы, с которыми мы столкнулись в настоящее время.

Сегодня предприятия, государственные организации и органы пограничной службы в том числе, активно внедряют современные программные решения по обеспечению информационной безопасности, обнаружению рисков и угроз в информационной инфраструктуре. Повсеместно расширяется применение средств технической и криптографической защиты.

На уровне государства закреплена важность обеспечения информационной и кибербезопасности военных объектов, промышленности, транспорта и энергетики, объектов электросвязи и здравоохранения.

Отдельным вопросом становится подготовка кадров в этой области, формирование у сотрудников понимания важности соблюдения правил информационной безопасности в повседневной работе.

Для эффективного решения задач в обеспечении защиты информации важно постоянное взаимодействие между заинтересованными структурами и тесная взаимосвязь науки и практики.

Уважаемые участники! Уверен, что в ходе конференции удастся обсудить вопросы и перспективы развития в сфере обеспечения комплексной защиты информации, обменяться передовым опытом по их решению.

Желаю всем успешной и плодотворной работы!

**Председатель государственного пограничного
комитета Республики Беларусь
генерал-лейтенант**



А.П.Лаппо

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

АКТУАЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОЮЗНОМ ГОСУДАРСТВЕ

МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ФОРМИРОВАНИЯ ТРЕБОВАНИЙ К ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Ю.К. ЯЗОВ, С.В. СОЛОВЬЕВ

*Федеральное автономное учреждение «Государственный научно-исследовательский институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю»,
г. Воронеж, Российская Федерация*

Сегодня в России действуют более 20 нормативных документов, содержащих требования по технической защите информации (ТЗИ) в информационных системах (ИС). Структура системы таких требований весьма обширна, поскольку они охватывают самые различные аспекты регулирования деятельности по защите информации, такие как формирование терминологии в предметной области, категорирование ИС и информационных ресурсов, построение систем защиты в функционирующих ИС и вновь создаваемых ИС в защищенном исполнении, создание средств защиты и контроля защищенности информации в ИС и др. [1]. Рассмотреть все эти аспекты в одном докладе не представляется возможным, поэтому в нем акцентировано внимание только на требованиях к эффективности ТЗИ в ИС.

Сегодня формирование требований по ТЗИ в ИС фактически не связывается с количественной оценкой эффективности защиты. При этом защита считается эффективной, если выполняются требования, установленные действующим нормативным правовым документом государственного регулятора или стандартами (международными или национальными), а неэффективной, – если эти хотя бы одно из требований не выполняются. Состав требований сформирован экспертно без каких-либо количественных обоснований достигаемой защищенности информации в ИС. Несомненным достоинством такого подхода является простота и ясность процедуры формирования требований. Однако ему присущи весьма существенные недостатки, к основным из которых относятся:

- наличие лишь опосредованной связи требований с оценками возможностей реализации угроз (по сути, угроза рассматривается как актуальная, если экспертно определено, что она реализуема в данной ИС и наносит значимый ущерб для обладателя информации);
- отсутствие учета фактора времени при задании требований;
- отсутствие какого-либо обоснования при соотнесении классов защищенности ИС и классов защиты, применяемых или подлежащих применению в ИС средств защиты информации;
- неопределенности, возникающие при попытке применения новых мер и средств защиты в интересах парирования новых угроз безопасности информации, не известных при создании нормативного документа, в соответствии с которым оценивается эффективность;
- неопределенности, которые могут возникать при настройках программных или программно-аппаратных средств и систем защиты (с вариативными настройками, как правило, не связываются установленные требования по ТЗИ в ИС) и т.д.

В этих условиях несомненно важной является разработка количественных методов обоснования требований по ТЗИ в ИС и, в частности, требований к эффективности ТЗИ, которые учитывали бы возможности реализации угроз в конкретных ИС и уровень наносимого при этом ущерба. Такие требования сегодня можно и целесообразно разрабатывать с использованием теории рисков при анализе возможностей реализации угроз безопасности информации без применения и с применением мер и средств защиты. В этом случае

требования должны формироваться путем установления предельных значений или требуемого значения показателя эффективности защиты, или предельно допустимого риска реализации рассматриваемой угрозы (совокупности угроз).

Вместе с тем сегодня фактически отсутствует подход к определению как требуемого значения показателя эффективности, так и предельно допустимого риска реализации угроз.

В данном докладе предлагается один из подходов к решению этого вопроса. Наиболее простой путь для определения предельных значений указанных параметров состоит в установлении их обладателем информации, возможно с градацией, например, по требуемым классам защищенности ИС. В этом есть резон, так как каждой ИС соответствует своя шкала ценностей обрабатываемой в ней информации, существенно зависящая не только от того, какая информация, подлежащая защите, хранится и обрабатывается в ИС, какие имеют место объемы и сроки ее обработки и т.д., но и от потребностей и интересов самого обладателя. Это, с одной стороны, приводит к значительному упрощению процедуры обоснования, но с другой – обуславливает необходимость разработки состоятельных, обоснованных и проверенных на практике применительно к разным ИС рекомендаций по реализации указанной процедуры.

Значительно более перспективным является подход к формированию *количественных требований* к эффективности защиты информации и к предельно допустимому риску реализации угроз. Именно этот подход рассматривается далее.

Соответствующий вариант структуры системы количественных требований к эффективности защиты информации и к предельно допустимому риску реализации угроз приведен на рисунке 1.

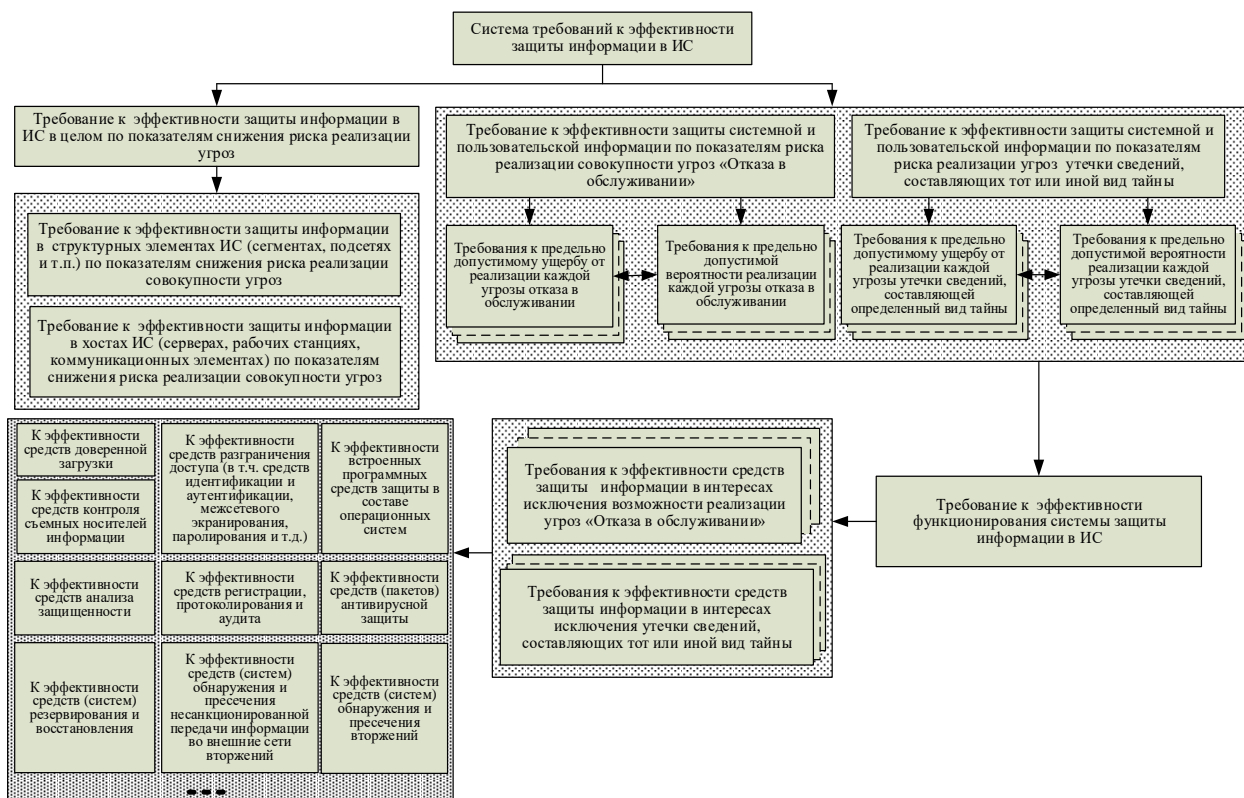


Рисунок 1. – Система требований к эффективности защиты информации в информационной системе (вариант)

Процедуры обоснования приведенной системы требований имеют определенные особенности, суть которых состоит в следующем.

1. Процедуры, как правило, являются иерархическими, осуществляемыми «сверху вниз», например, начиная с требований к эффективности ЗИ в течение всего жизненного цикла ИС и заканчивая этапом вывода ее из эксплуатации, или начиная с требований

к эффективности защиты информации в ИС в целом и заканчивая требованиями к эффективности защиты информации, содержащейся в системных файлах и файлах с пользовательской информацией и т.д.

2. В них должна быть обеспечена преемственность подхода к заданию требований по эффективности в части их дифференциации по классам защищенности ИС и средств вычислительной техники (СВТ) в их составе.

3. Процедуры обоснования требований существенно зависят от класса угроз безопасности, которые имеют место в защищаемой ИС, в частности, существенно различаются для угроз «отказа в обслуживании» (угроз вывода из строя, нарушения функционирования ИС, операционных систем хостов ИС – серверов, рабочих станций, функционирования коммуникационных элементов ИС – маршрутизаторов, коммутаторов, концентраторов, повторителей и т.д.) и угроз утечки информации ограниченного распространения. Это связано, прежде всего, с определением предельно допустимых показателей возможности нарушения функционирования ИС. Сегодня фактически отсутствует подход к заданию количественных требований к эффективности защиты информации, когда нарушение целостности или доступности этой информации приводит к нарушению функционирования ИС. Далее излагается один из путей решения этого вопроса на основе использования теории риска.

Формирование количественных требований к эффективности защиты ИС от угроз отказа в обслуживании, то есть к заданию требуемого значения одного из следующих показателей эффективности:

при использовании безотносительного показателя эффективности:

$$\eta_{dif}^{(mpe\delta)}(T) = R_u^{(0)}(T) - R_u^{(\delta on)}(T); \quad (1)$$

при использовании относительного показателя эффективности:

$$\eta_{rel}^{(mpe\delta)}(T) = R_u^{(\delta on)}(T) / R_u^{(0)}(T), R_u^{(0)}(T) > 0; \quad (2)$$

при использовании относительного разностного показателя эффективности:

$$\eta_{reldif}^{(mpe\delta)}(T) = |R_u^{(0)}(T) - R_u^{(\delta on)}(T)| / R_u^{(0)}(T), R_u^{(0)}(T) > 0, \quad (3)$$

где $R_u^{(0)}(T)$ – риск, возникающий для ИС при реализации угрозы отказа в обслуживании при отсутствии мер защиты за период оценки T , равный произведению математического ожидания возможного ущерба ($\overline{\zeta_u^{(0)}}$) от реализации u -й угрозы на вероятность $P_u^{(0)}(t)$ ее реализации за заданное время без мер защиты,

$$R_u^{(0)}(t) = \overline{\zeta_u^{(0)}} \cdot P_u^{(0)}(t), \quad (4)$$

где $R_u^{(\delta on)}(T)$ – предельно допустимое значение риска, определяемое при организации защиты от угрозы отказа в обслуживании.

Если при отсутствии мер защиты риск нарушения функционирования близок к единице, то формулы значительно упрощаются:

$$\eta_{dif}^{(mpe\delta)}(T) = \eta_{reldif}^{(mpe\delta)}(T) = 1 - R_u^{(\delta on)}(T); \quad \eta_{rel}^{(mpe\delta)}(T) = R_u^{(\delta on)}(T). \quad (5)$$

Весьма существенным обстоятельством при задании требуемых значений показателей эффективности является учет фактора времени, то есть необходимость определения периода

времени, в течение которого должна сохраняться эффективность защиты, как это принято в теории надежности [2, 3]. Таким периодом может быть, например, период времени до пересмотра состава актуальных угроз и мер защиты в связи с появлением новых угроз, изменением условий функционирования ИС, состава и характеристик ее аппаратного обеспечения и др. Это может быть и плановый период времени: для одних ИС это может быть один год, для других три и даже пять лет. Вместе с тем отказ от учета фактора времени приводит к несостоятельности требований, предъявляемых к эффективности защиты информации в ИС, если эти требования не направлены на исключение возможности реализации угроз.

Таким образом, при формировании требований к эффективности защиты ИС от угрозы отказа в обслуживании достаточно задать предельно допустимое значение риска реализации такой угрозы $R_u^{(\partial on)}(T)$ за период оценки T . Далее задаются требования к предельно допустимому среднему ущербу $\left(\overline{\zeta_u^{(\partial on)}}\right)$ и к предельно допустимой вероятности реализации угрозы отказа в обслуживании $P_u^{(\partial on)}(T)$ для ИС с учетом требуемого класса защищенности для нее так, чтобы

$$\overline{\zeta_u^{(\partial on)}}(k) \cdot P_u^{(\partial on)}(k, T) \leq R_u^{(\partial on)}(k, T), k = \overline{1, K}, \quad (6)$$

где k – номер класса защищенности, заданный для данной ИС, при этом самая высокая защищенность соответствует первому классу ($k = 1$), а самая низкая – последнему ($k = K$);

K – общее количество классов защищенности, установленное государственным регулятором или в ведомстве.

Если установлен предельно допустимый ущерб от угрозы отказа в обслуживании для первого класса $\overline{\zeta_u^{(\partial on)}}(1)$, то для $k > 1$ имеет место соотношение:

$$\overline{\zeta_u^{(\partial on)}}(k) = \varepsilon(k) \overline{\zeta_u^{(\partial on)}}(1), \varepsilon(k) \geq 1, \quad (7)$$

где $\varepsilon(k)$ – коэффициент увеличения размера предельно допустимого ущерба от угрозы отказа в обслуживании для k -го класса защищенности по сравнению с первым, при этом, как правило, полагается, что для первого класса защищенности ущерб считается неприемлемым, то есть $\varepsilon(1) = 1$.

В основе предлагаемого подхода к формированию требования к предельно допустимой вероятности реализации угрозы отказа в обслуживании лежит идея о том, что нарушение функционирования ИС одинаково опасно для обладателя и пользователей ИС независимо от того, произошло ли оно из-за преднамеренного воздействия на программно-аппаратные элементы ИС или из-за отказа этих элементов в условиях отсутствия указанного воздействия, то есть из-за возникновения неисправностей, сбоев, ошибок в настройках, ошибок пользователей и т.д., характеризующихся таким понятием как «функциональная надежность» ИС [2], которая оценивается вероятностью безотказной работы [3] или в соответствии с [2] вероятностью безошибочного выполнения процесса, то есть функционирования ИС. Если учесть, что сегодня требования к функциональной надежности задаются соответствующими стандартами, например, стандартами [4], то имеется возможность обосновать предельно допустимую вероятность реализации угрозы отказа в обслуживании. При таком подходе учитывается, является ли источник u -й угрозы внутренним или внешним, в соответствующей модели процесса реализации угрозы. Если источников (внутренних или внешних) много и ими используется один и тот же способ реализации угрозы, то это учитывается в интенсивности возникновения угрозы.

Более сложной оказывается процедура задания требований к эффективности защиты элементов ИС (серверов, рабочих станций, коммутационных устройств и т.п.) от угрозы нарушения их функционирования. При этом полагается, что ИС выходит из строя, когда:

1) выходит из строя любой из некоторого множества элементов ИС, относящихся к критически важным, то есть нарушение функционирования любого из этих элементов неизбежно приводит к отказу в обслуживании всей ИС;

2) выходит из строя любая из некоторых совокупностей элементов ИС, при этом в каждой совокупности выходят из строя все входящие в нее элементы, то есть нарушение функционирования ИС происходит, когда деструктивное воздействие происходит на все элементы хотя бы одной из критически важных совокупностей элементов ИС.

Так как последствия примерно одинаковы, независимо от того, какой критически важный элемент выводится из строя, то требования предъявляются только к предельно допустимой вероятности вывода из строя каждого критически важного элемента.

В первом из указанных случаев сначала определяются предельно допустимые значения вероятности $P_{ud}^{(don)}(k, n_{kr} \geq 1, T)$ того, что в результате преднамеренного деструктивного воздействия выйдет из строя хотя бы один из критически важных элементов ИС, которая с учетом класса защищенности определяется из уравнения:

$$P_{ud}^{(don)}(k, n, T) \leq 1 - \sqrt[N_{kp}]{1 - \varepsilon(k) \cdot P_{func}^{(don)}(T)}, \quad \varepsilon(k) \geq 1, k = \overline{1, K}. \quad (8)$$

Во втором из указанных случаев сначала определяются предельно допустимые значения вероятности $P_{ud}^{(don)}(S_{kr}, T)$ того, что в результате преднамеренного деструктивного воздействия выйдет из строя хотя бы одна из критически важных совокупностей элементов ИС, которая без учета класса защищенности определяется из уравнения:

$$P_{ud}^{(don)}(S_{kr}, T) = 1 - \prod_{s=1}^{S_{kr}} \left[1 - \prod_{n=1}^{N_s} P_{ud}^{(don)}(n, T) \right] \leq P_{func}^{(don)}(T), \quad (9)$$

где N_s – общее количество элементов, входящих в s -ю критически важную совокупность элементов ИС, $s = \overline{1, S_{kr}}$.

Далее с учетом класса защищенности ИС это уравнение преобразуется к виду:

$$1 - \prod_{s=1}^{S_{kr}} \left\{ 1 - \left[P_{ud}^{(don)}(k, T) \right]^{N_s} \right\} \leq \varepsilon(k) P_{func}^{(don)}(T), \quad \varepsilon(k) \geq 1, k = \overline{1, K}. \quad (10)$$

Аналогичным образом могут быть детализированы требования, предъявляемые к предельно допустимой вероятности нарушения целостности или доступности системных файлов в конкретном программно-аппаратном элементе ИС или пользовательских файлов, без которых перестает нормально функционировать прикладное ПО, что для пользователя равносильно выводу из строя самой ИС.

Данный подход может быть расширен и на случай задания требования по защите конфиденциальной информации, то есть к информации, содержащей сведения, составляющие тот или иной вид тайны (служебной, коммерческой, профессиональной, личной) или персональные данные, кроме государственной тайны, что регулируется иным образом и здесь не рассматривается. В данном случае также должен быть обеспечен дифференцированный подход к требованиям по эффективности защиты в зависимости от того, какие сведения защищаются от утечки. При задании соответствующих требований должен проводиться анализ обрабатываемой или подлежащей обработке информации на предмет отнесения

содержащейся в ней сведений к тому или иному виду тайны или персональным данным. Соответственно, разделяется все множество файлов с пользовательской информации ограниченного доступа по видам тайн.

При этом оказывается важным то, к кому и в какие сроки попадут эти сведения, а также, насколько быстро они устаревают, что, как правило, весьма сложно оценить. Все это приводит к тому, что при формировании требований к эффективности ТЗИ могут быть использованы два варианта оценки. В первом полагается, что любая утечка конфиденциальной информации приводит к недопустимому ущербу, а требования к эффективности ее защиты формируются только применительно к предельно допустимой возможности ее утечки (перехвата, копирования, несанкционированной передачи и т.д.). Во втором варианте полагается, что недопустимый ущерб имеет место в ИС с первым классом защищенности, а риски для других классов защищенности снижаются путем умножения на соответствующие коэффициенты (возможно пропорционально числу, соответствующему классу защищенности).

Пусть имеет место первый вариант и риск утечки любой конфиденциальной информации считается недопустимым. Тогда в зависимости от того, к какому виду тайны относятся сведения, раскрываемые в результате возможной утечки информации, определяются предельно допустимые значения вероятностей $P_{uv}^{(\partial on)}(f_{conf}, k, T)$ реализации угрозы утечки информации в ИС с классом защищенности k , соответствующей v -му виду тайны и содержащейся в файле с номером f_{conf} . Первый вариант состоит в том, что предельно допустимая вероятность утечки при каждой попытке реализации соответствующей угрозы не должна превышать предельно допустимой вероятности $P_{ud}^{(\partial on)}$ выхода из строя элемента ИС, где обрабатывается эта информация, при этом обладатель выбирает тот вид тайны, для защиты которой предъявляется наиболее высокие требования (пусть это соответствует виду тайны с номером $v = 1$), то есть:

$$P_{u,1}^{(\partial on)}(f_{conf}, k) \leq P_{ud}^{(\partial on)}, \quad (11)$$

где $P_{uf1}^{(\partial on)}$ – предельно допустимая вероятность того, что в каждой попытке будет реализована угроза утечки информации, содержащей сведения, относящиеся к виду тайны ($v = 1$), для которого устанавливаются наиболее жесткие требования по защите.

Затем устанавливаются коэффициенты, определяющие изменение требований применительно к иным видам тайн $\zeta_v, v = 1, 2 \dots V$. При этом самые высокие требования соответствуют наиболее важной информации, тогда $\zeta_1 = \zeta_{\min}$, (как правило, полагается, что $\zeta_{\min} = 1$, и $\zeta_v = \zeta_{\max} \geq 1$), а предельно допустимая вероятность того, что в каждой попытке будет реализована угроза утечки информации, содержащей сведения, относящиеся к v -му виду тайны ($v > 1$), для которого устанавливаются наиболее жесткие требования по защите, рассчитывается следующим образом:

$$P_{ufv}^{(\partial on)} = \zeta_v \cdot P_{uf1}^{(\partial on)}, \quad \zeta_v > 1, v = 2, 3 \dots V. \quad (12)$$

Если рассматривать требования по защите N_v файлов с конфиденциальной информацией с v -м видом тайны, имеющих в хосте ИС, для которой установлен k -й класс защищенности, то предельно допустимая вероятность $P_{ufv}^{(\partial on)}(k, T)$ рассчитывается из неравенства:

$$P_{ufv}^{(don)} \leq \frac{1}{T \cdot \lambda_{ufv}} \ln \left[\frac{1}{1 - N_v \sqrt{\frac{P_{ufv}^{(don)}(N_v, k, T)}{\varepsilon(k)}}} \right], \quad (13)$$

где λ_{uf} – интенсивность попыток реализации угрозы относительно f -го файла с информацией, содержащей сведения, относящиеся к v -му виду тайны.

Если файлов с конфиденциальной информацией много и сложно проводить оценки возможностей реализации угроз ее утечки применительно ко всем таким файлам, то можно воспользоваться приемом, при котором полагается, что с единичной вероятностью будет выполняться несанкционированное действие относительно любого из файлов с конфиденциальной информацией, если нарушителем или иницированным им процессом получен доступ в операционную среду хоста ИС. При этом требование задается относительно предельно допустимой вероятности $P_{fvOS}^{(don)}(k, T)$ получения несанкционированного доступа в операционную среду, то есть должно выполняться неравенство:

$$P_{fvOS}^{(don)}(k, T) \leq P_{ufv}^{(don)}(k, T). \quad (14)$$

Если имеет место вариант, при котором полагается, что для классов защищенности, выше первого, риск реализации угрозы не является неприемлемым, то для этих классов ($k > 1$) устанавливаются предельно допустимые значения рисков путем введения соответствующих коэффициентов следующим образом:

$$R_{fvOS}^{(don)}(k, T) \leq \gamma(k) \cdot R_{ufv}^{(don)}(1, T), k > 1, \quad (15)$$

где $\gamma(k)$ – коэффициент снижения риска реализации угроз получения несанкционированного доступа в операционную среду для ИС с классом защищенности $k > 1$.

Таким образом могут быть определены количественные требования к эффективности защиты защищаемой информации в ИС от угроз, реализуемых путем несанкционированного доступа к ней.

Сложности в реализации данного подхода, конечно, имеются, однако они могут быть преодолены путем:

разработки комплекса математических моделей процессов реализации угроз безопасности информации в различных информационных системах с учетом фактора времени без мер защиты и в условиях их применения;

разработки математических моделей задания количественных требований к системам и средствам ЗИ в ИС (в том числе к составляющим элементам ИС – подсетям, серверам, АРМ и т.д.);

разработки комплекса стандартов по моделям и алгоритма количественной оценки возможностей реализации угроз безопасности информации в различных ИС без мер защиты и в условиях их применения и задания требований по ЗИ;

создания программных комплексов, обеспечивающих в автоматизированном режиме оценку возможностей реализации угроз безопасности информации в ИС.

Вместе с тем следует подчеркнуть, что сегодняшняя ориентация на экспертные методы оценки и обоснования требований по защите информации в ИС – это тупиковый путь. Необходимо переходить к количественным методам.

Литература

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. Шубинский, И.Б. Функциональная надежность информационных систем. Методы анализа / И.Б. Шубинский. – Ульяновск: Областная типография «Печатный двор», 2012. – 296 с., ил. ISBN 978-5-7572-0327-0.
3. Половко, А.М. Основы теории надежности. – 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2006. – 704 с.: ил. ISBN 5-94157-541-6.
4. ГОСТ Р 27.003. Надежность в технике управление надежностью. Руководство по заданию технических требований к надежности. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 14 декабря 2011 г. № 1490-ст.

Авторы

1. Язов Юрий Константинович, доктор технических наук, профессор, главный научный сотрудник управления ФАУ «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю», г. Воронеж, Россия. Email: yazoff_1946@mail.ru.
2. Соловьев Сергей Вениаминович, кандидат технических наук, доцент, заместитель начальника ФАУ «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» по информационной безопасности, г. Воронеж, Россия. Email: solovev@gniii.ru

ИМПОРТОЗАМЕЩЕНИЕ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ – КОМПЛЕКСНЫЙ ПОДХОД К ЗАЩИТЕ ИНФОРМАЦИИ

А.В. БЕЛЕВИЧ, С.В. НАЛИВАЙКО, С.Н. СИРИСЬКО

*Общество с ограниченной ответственностью «СБК групп ИТ»,
г. Минск, Республика Беларусь*

Импортозамещение для Беларуси давно стало приоритетной задачей. До 2022 г. она была на уровне «планового», но лишь «желательного» движения. В настоящее время оно вышло на уровень острой необходимости, когда в области информационных технологий от скорости разработки и внедрения может зависеть не только конкурентоспособность отдельных предприятий, но и траектория развития отраслей на ближайшие десятилетия.

В таких обстоятельствах особую величину приобретают собственные разработки организаций и отечественные программные продукты. Удовлетворение потребностей зарубежными программами за многие годы не позволяло отечественным конкурентам занять свое место и развиваться быстрее. Из-за этого для местных разработчиков практически отсутствовала национальная программная база, а соответственно, не было направлений обучения для работы с ее использованием в контексте одного из этапов развития интеллектуального потенциала нашей страны. А ведь сейчас имеет значение даже стадия готовности отечественных программных продуктов для внедрения, и чем она выше, тем лучше. Стоит признать, что импорт готовых решений, когда он возможен, конечно, может ускорять процессы в организации, которые он опосредует, но как минимум параллельно с этим, собственные разработки, принадлежащие резидентам Беларуси, должны поддерживаться финансово, интеллектуально и иметь приоритет в закупках. Это будет снижать зависимость от зарубежного ПО и повышать интеллектуальную базу наших разработчиков, увеличивать их доходы, создавать вокруг себя экосистему, дистрибьюторскую сеть и как следствие – увеличивать налоговые поступления в бюджет страны. Ускорить достижение целей импортозамещения можно также, используя программные коды, распространяемые по свободным лицензиям, и создавая все больше выгодных условий для создания стартапов и технопарков в стране.

Считаем, стало бы отличной практикой до начала эксплуатации систем организациям-заказчикам программ и разработчикам по умолчанию внедрять стандарты и методики, способные выявлять угрозы, скрытые коды для целей обеспечения информационной безопасности. Либо устанавливать корпоративное правило: перед началом использования новой программы обращаться за аудитом кода к независимым специализированным организациям по обеспечению информационной безопасности.

В любой организации важнейшим аспектом работы с информацией, базами данных является их защита от утечки, неограниченного доступа, некорректного предоставления и сбоев при ее обработке. В частности, это касается электронного документооборота, бухгалтерских операций, управления сбытом, кадрами, закупками, производством и многих других процессов. В организациях, особенно полного цикла, вышеизложенное имеет жизненно важное значение, ведь любой сбой, остановка, утечка несет не только финансовые убытки и репутационные риски, но и угрозу промышленной безопасности, шантажа и раскрытия закрытой информации. Поэтому обеспечение плановой, бесперебойной, а в современных реалиях автоматизированной работоспособности организаций по данным направлениям следует относить к информационной безопасности особой значимости.

Программный продукт, который позволяет крупным предприятиям обеспечивать автоматизацию этих процессов называют ERP-система (Enterprise Resource Planning – планирование ресурсов предприятия).

В Республике Беларусь до недавнего времени ниша таких программ была занята преимущественно такими представителями как: SAP (Германия), Vaan (Нидерланды), Oracle (США), Microsoft Dynamics 365 (США). В 2022 году указанные Лицензиары прекратили выдачу новых лицензий на использование на территории Беларуси и России. По сегодняшний день лицензиаты остаются как минимум без технической поддержки и обновлений, а как максимум без права использовать данные программы.

Помимо вышеуказанного предполагается, что они могут содержать в себе так называемый спящий код, закрытые библиотеки, функционал которых не известен достоверно и не используется пользователем. Какую реальную роль они выполняют при эксплуатации системы? Все это создавало уязвимость и зависимость для местных организаций, а вдобавок большие суммы за техническую поддержку и роялти уходили за рубеж. Что остается делать местным компаниям если не импортировать снова аналоги указанных ERP-систем?

В Республике Беларусь единственной, полностью отечественной ERP-системой полного цикла является «СБК-предприятие». Она зарегистрирована в Республике Беларусь 02.04.2009 за № 072 в Национальном центре интеллектуальной собственности и в реестре Минцифры РФ за № 3048 в 2017 году. Группа компаний «СБК» ведет ее разработку и точечное внедрение с 1995 г. Данная платформа показала свою способность конкурировать по функционалу и надежности с такими зарубежными гигантами как SAP и ORACLE. Обладая отдельными, существенными техническими преимуществами она полностью готова к внедрению и создает лучшее предложение в рынке по соотношению «цена – качество».

Безопасность использования «СБК-предприятие» обеспечивается несколькими способами:

- ограничение внешнего доступа к инфраструктуре организации;
- ограничение доступов паролем к системе при входе;
- ограничение доступа к разделам данных в зависимости от определенных потребностей сотрудников после входа в систему;
- не используются заимствования;
- отсутствует «спящий код» и потенциально шпионское ПО, что подтверждается использованием открытых библиотек;
- при использовании веб-версии предполагает удаленный сервер, что обеспечивает дополнительную сложность для злоумышленников;
- при использовании мобильного приложения возможно задействовать аппаратные защитные функции для доступа к нему;
- технологии, реализуемые на платформе «СБК-предприятие», предусматривают средства поддержки принятия решений на основе анализа аналогий (с использованием искусственного интеллекта и технологий машинного обучения), а также поддерживают реализацию смарт-контрактов (с применением технологий «blockchain») [1];
- при работе сервера с использованием процессоров «Эльбрус» производства АО «МЦСТ» (РФ) обеспечивается аппаратная защита обрабатываемых данных, предусмотренная архитектурой изделий.

О последнем подробнее, поскольку эта уникальность характеризует «СБК-предприятие» как единственную ERP-систему в мире, способную работать на процессорах Российского производства.

28.04.2021 изготовителем процессоров АО «МЦСТ» был выдан сертификат совместимости № 3, который подтверждает вышеуказанный факт. Ключевая особенность микропроцессоров «Эльбрус» – наличие так называемого защищенного режима. Он устроен сложнее традиционных процессоров, поэтому большинство вирусов в нем не работают. Сохранение регистра происходит аппаратно и не доступно для прикладного кода, но для максимальной защиты, при использовании защищенного режима, будет производиться тегирование данных в памяти процессора. В центральной памяти используется технология безопасных вычислений, она выявляет ошибки, которые можно использовать как уязвимости. Процессор сам их обнаруживает и блокирует на аппаратном уровне [2].

Совместное использование данной программы с такими процессорами позволяет создавать программно-аппаратные комплексы управления предприятием (далее – ПАК УП), серверы, персональные компьютеры для поставки организациям различного масштаба, где таким образом будет обеспечиваться высочайшая безопасность использования данных. При этом замена имеющегося оборудования не понадобится – ПАК УП может дополнять текущую инфраструктуру, а «СБК-предприятие» может использоваться с любыми традиционными на сегодняшний день серверами, ПК и совместима с любым программным обеспечением.

Настолько защищенный доступ к данным и такой подход к защите информации уже сегодня может позволить не просто отказаться от импортных ERP-систем, но и обойти их конкурентно: качественно и экономически. Он также может обеспечить надежную эксплуатацию систем и баз данных на самых ответственных направлениях автоматизации производства и планирования ресурсов любых организаций.

Из всего вышеуказанного следует, что необходимо развивать собственные программные продукты за счет поддержки как местных стартапов, так и обеспечения заказами местных IT-компаний, чем будут защищаться квалифицированные кадры от утечки за рубеж и будет развиваться интеллектуальная база специалистов нашей страны.

Учитывая острую потребность крупных организаций в отечественной, безопасной ERP-системе существует реальная возможность создать целую экосистему вокруг нее с большим количеством сотрудников и направлениями разработки программ, способных работать на процессорах российского производства «Эльбрус», поскольку имеется опыт в адаптации программ для работы с их использованием.

Развитие собственных технологий, а не обучение иностранным создает более надежную базу для дальнейшего роста национального интеллектуального потенциала и минимизирует риски, связанные с импортом и заимствованием.

Литература

1. А.Ф. Страхов д.т.н., проф., О.А. Страхов к.т.н., доц., А.В. Белевич, С.В. Наливайко: Информационные технологии в ситуационном управлении промышленным предприятием, Москва, Общетехническая (ОТ) серия, 2011 г.

2. Ким А.К., Волконский В.Ю., Груздов Ф.А., Сахин Ю.Х., Семенихин С.В. Защищенное исполнение программ на базе аппаратной и системной поддержки архитектуры «Эльбрус» [Электронный ресурс]. V Международная научно-практическая конференция «Современные информационные технологии и ИТ-образование», Москва, МГУ, 2010 г. URL: <http://mcst.ru/publikacii-mcst-s-2004goda> (дата обращения: 25.04.2023 г.)

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КРИПТОЛОГИИ

Ю.С. ХАРИН, И.Б. БЕРЕЖНОЙ

*Белорусский государственный университет,
НИИ прикладных проблем математики и информатики,
г. Минск, Республика Беларусь*

Введение

История развития криптологии, составными частями которой являются криптография и криптоанализ, сложна и включает 3 этапа [1]:

Этап 1 (с древних времен до 1949 г.) – этап докомпьютерной криптологии.

Этап 2 (1949–1976 гг.) принято отсчитывать с момента публикации 60-страничной статьи «Теория в секретных системах» американским математиком-прикладником К. Шенноном. Следует отметить, что исторически первым строгое математическое обоснование того, что симметричные алгоритмы шифрования с одноразовыми ключами являются абсолютно стойкими, дал еще в июне 1941 г. академик АН СССР В.А. Котельников. Однако данное обоснование было опубликовано в секретном отчете и на протяжении всего XX века так и не было представлено в открытой печати [2].

Этап 3 (1976 г. – настоящее время) принято отсчитывать с момента публикации статьи У. Диффи и М. Хеллмана об асимметричных (двухключевых) алгоритмах шифрования.

Статья посвящена современным актуальным проблемам криптологии.

1. Источники случайности (энтропии)

В криптографии генерация случайности сводится к задаче генерации равномерно распределенной случайной последовательности (РРСП) $x_t \in \{0,1\}$, $t = 1, 2, \dots$, которая определяется двумя базовыми свойствами:

C_1) для любого n и случайных индексов $1 \leq t_1 < \dots < t_n$ случайные величины x_{t_1}, \dots, x_{t_n} независимы в совокупности;

C_2) для любого номера t случайная величина x_t имеет равномерное распределение: $P\{x_t = a\} = 1/2$, $a \in \{0,1\}$.

Генерация РРСП представляет собой важную задачу не только для генерации «гаммы» в поточных криптосистемах, но и в других системах криптографической защиты информации для выработки ключей и векторов инициализации, одноразовых чисел (называемых в англоязычной литературе Nonce) в криптографических протоколах и схемах ЭЦП.

Генераторы РРСП можно разделить на следующие подмножества: 1) аппаратные генераторы; 2) программно-аппаратные генераторы; 3) программные генераторы.

Аппаратные (физические) генераторы РРСП позволяют вырабатывать случайные последовательности на основе физических процессов в объектах, параметры которых меняются хаотически (например, использование полупроводникового лазера позволяет вырабатывать РРСП на скоростях от 160 Гбит/с [3], а шумовой диод ND103L производства Республики Беларусь – на скорости около 0,5 Мбит/с [4]). Теоретически такие процессы непредсказуемы, однако на практике на хаотические процессы постоянно влияют окружающая среда и измерительная аппаратура. Отсюда проистекают **недостатки аппаратных генераторов**: необходимость постоянного контроля свойств получаемой последовательности и невозможность репликации последовательности на другом устройстве классической компьютерной архитектуры.

В целях устранения необходимости в постоянном контроле аппаратных генераторов применяются программно-аппаратные генераторы, в которых происходит дополнительная программная обработка данных с аппаратного источника, что позволяет получить лучшие статистические характеристики и увеличить скорость генерации РРСП. Однако **проблема**

репликации последовательности ограничивает сферу применения и для программно-аппаратных генераторов.

Широко распространенной альтернативой аппаратным генераторам РРСП стало использование программных генераторов, к которым предъявляются следующие два требования «практической криптостойкости» (т.е. криптостойкости при условии «разумных» ограничений у противника на время и вычислительные ресурсы для анализа перехваченного сообщения): 1) выходную последовательность генератора невозможно отличить от РРСП на основании определенного набора статистических тестов; 2) знание некоторого отрезка выходной последовательности не позволяет предсказать последующие элементы последовательности.

Последовательность («гамма»), полученная из такого программного генератора, называется псевдослучайной последовательностью (ПСП). Следует отметить, что так как ПСП программных генераторов полностью определяются начальным значением (называемым в англоязычной литературе seed), то **недостатком таких генераторов является проблема источника энтропии для формирования случайного равномерно распределенного значения seed.** Другими словами, обеспечение «практической криптостойкости» программного генератора ПСП происходит за счет не только математических, но и физических методов, хотя и в сравнительно малом объеме.

Существующие криптографические генераторы ПСП принято классифицировать в два подмножества [1, 5]: 1) простые (элементарные) генераторы, использующие единственную псевдослучайную последовательность для генерации выходной последовательности: а) конгруэнтные генераторы; б) генераторы с регистром сдвига; в) генераторы Фибоначчи; г) генераторы на основе односторонних функций; д) генераторы, основанные на проблемах теории чисел; 2) составные генераторы, использующие несколько «простейших» псевдослучайных последовательностей для генерации выходной последовательности: а) фильтрующие и комбинирующие генераторы; б) композиционные генераторы (каскады); в) генераторы с динамическим изменением законов рекурсии; г) **генераторы с дополнительной памятью [6].**

2. Статистическое тестирование криптографических генераторов случайных и псевдослучайных последовательностей

Для определения статистических свойств выходных последовательностей криптографических генераторов ПСП используются наборы (так называемые батареи) статистических тестов, каждый из которых вычисляет вероятность (Р-значение) события, состоящего в том, что «генератор истинно случайных чисел» выработает последовательность с определенной статистикой «хуже», чем у проверяемой. Другими словами, батарея тестов выдает вектор вероятностей события, состоящего в том, что исследуемая последовательность близка к РРСП.

Каждый статистический тест представляет собой решающее правило $d = d(X) \in \{0,1\}$ для проверки гипотезы H_0 о том, что исследуемая последовательность $X = \{x_1, \dots, x_T\}$ является равномерно распределенной случайной последовательностью против альтернативной гипотезы $H_1 = \bar{H}_0$. Для исследуемой последовательности вычисляется некоторая статистика, распределение вероятностей которой при истинной гипотезе H_0 известно. На основании значения статистики или (Р-значения) гипотеза H_0 принимается либо отклоняется.

На текущий момент существует ряд известных батарей тестов: DieHarder [7], NIST STS [8], gjrands [9], testU01 [10].

Проведенный в [1] обзор существующих статистических тестов выявляет следующие **недостатки**: 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 вообще не фиксируют

семейство альтернатив H_1 ; 3) многие тесты не имеют оценок мощности $w = P\{d = 1/H_1\}$; 4) при включении нескольких тестов в батарею не удается учесть их вероятностную зависимость и оптимизировать «составной» тест.

Следует еще отметить, что в марте 2022 г. вышла статья [11], авторы которой обнаружили прямые ошибки в реализации одного из тестов батареи NIST STS, а также проблемы с вычислением P-значений у данной батареи на последовательностях большой длины (≈ 1 Гбит). В связи с этим в апреле 2022 г. NIST объявил [12] о начале процесса пересмотра собственной батареи и специально обратил внимание на непригодность текущей версии для оценивания криптографических генераторов ПСП.

Для преодоления указанных недостатков предлагается строить статистические тесты s -мерной равномерности для заданных семейств альтернатив H_1 с использованием энтропийных профилей [13, 14] и строить асимптотические оценки мощностей известных NIST-тестов [15].

Существующие статистические тесты и построенные на их основе батареи выходных последовательностей криптографических генераторов обладают еще одним недостатком, приводящим к следующему парадоксу: при увеличении длины $T \rightarrow +\infty$ наблюдаемых последовательностей реально существующих генераторов вероятность принятия альтернативы H_1 стремится к единице: $w_T \rightarrow 1$. Иначе говоря, «увеличением длины проверяемой последовательности T можно забраковать любой реальный генератор».

Объяснение этого парадокса состоит в следующем. Реальные генераторы не идеальны, они отклоняются от гипотезы H_0 по своему вероятностному распределению на некоторую величину $\varepsilon \neq 0$. Все тесты, включаемые в батареи тестов, как известно, обладают оптимальным свойством проверки простой гипотезы H_0 против сложной альтернативы ($H_1 = \bar{H}_0$) – свойством состоятельности: $w_T ::= P\{d = 1/H_1\} \rightarrow 1$. Таким образом, этот парадокс порожден некорректностью математической модели нулевой гипотезы H_0 . Для того чтобы избежать парадокса, гипотеза H_0 должна быть сложной: она должна задавать величину допуска ε отклонений от идеальной модели РПСИ. Приведем пример сложной гипотезы об s -мерном равномерном распределении двоичной случайной последовательности. Обозначим: $V = \{0, 1\}$ – двоичный алфавит, $p_{J_1^s} = P\{x_1 = j_1, \dots, x_s = j_s\}$, $J_1^s = (j_1, \dots, j_s) \in V^s$, –

s -мерное распределение вероятностей; $\mathbf{P} = \left\{ p = (p_{J_1^s}) : p_{J_1^s} \geq 0, \sum_{J_1^s \in V^s} p_{J_1^s} = 1 \right\}$ – множество всевозможных s -мерных распределений вероятностей;

$$\mathbf{P}_0^{(\varepsilon)} = \left\{ p \in \mathbf{P} : \sum_{J_1^s \in V^s} \left(p_{J_1^s} - \frac{1}{2^s} \right)^2 \leq \varepsilon^2 \right\}.$$

Сложная гипотеза об s -мерной равномерности:

$$H_0^{(\varepsilon)} = \left\{ p = (p_{J_1^s}) \in \mathbf{P}_0^{(\varepsilon)} \right\}.$$

Отметим, что при $\varepsilon \rightarrow 0$ получаем ранее рассмотренную простую гипотезу H_0 :

$$H_0^{(\varepsilon)} \rightarrow H_0.$$

Заметим еще, что при $s = 1$ гипотеза $H_0^{(\varepsilon)}$ принимает вид:

$$H_0^{(\varepsilon)} = \left\{ \left| \mathbb{P}\{x_t = 1\} - \frac{1}{2} \right| = \left| \mathbb{P}\{x_t = 0\} - \frac{1}{2} \right| \leq \frac{\varepsilon}{\sqrt{2}} \right\}.$$

Удается построить критерий обобщенного отношения правдоподобия для проверки сложных гипотез $H_0^{(\varepsilon)}$, $H_1 = \bar{H}_0^{(\varepsilon)}$.

3. Искусственные нейронные сети и машинное обучение в криптологии

Нейронные сети и машинное обучение составляют основу искусственного интеллекта. В сжатом виде в истории развития искусственных нейронных сетей (ИНС) можно выделить 3 этапа. **Этап I** (1940–1960 гг.) развивался под лозунгом «кибернетика» и был направлен на построение математической модели биологического нейрона в работах McCulloch, Pitts (1943 г.), Hebb (1949 г.), Rosenblatt (1958 г.). **Этап II** (1961–1990 гг.) развивался под лозунгом 1-слойных и 2-слойных ИНС и был направлен на разработку алгоритмов их обучения (Rummelhart, 1986 г.). **Этап III** (1991 г. – настоящее время) развивается под лозунгом «deep learning – глубокое обучение многослойных нейронных сетей».

Отметим, что теория ИНС базируется на решенной в 1957 г. академиком А.Н. Колмогоровым 13-ой проблемы Гилберта о композициях функций.

Анализ литературы позволяет выявить следующие направления использования ИНС и машинного обучения в решении актуальных задач криптологии: конструирование криптосистем на основе ИНС; классификация зашифрованного трафика; стеганоанализ; криптоанализ алгоритмов шифрования; криптоатаки на основе ИНС и машинного обучения; обнаружение вторжений и аномалий в сетях; обнаружение и анализ вредоносных.

В 1991 г. основатель RSA Р. Райвест на конференции ASIACRYPT'1991 представил приглашенный доклад «Криптография и машинное обучение», в котором впервые была указана необходимость использования ИНС в криптографии. В качестве примера использования ИНС в криптологии приведем информацию о результатах, полученных М.М. Alani [16]: успешно выполнен криптоанализ алгоритма DES на основе выборки 2^{11} пар (и 3-DES на основе выборки 2^{12} пар) «открытый текст – шифртекст» с одним и тем же ключом при затратах машинного времени 51 мин (72 мин) с использованием 4-слойной нейронной сети (256 нейронов в первом слое). Атака имеет цель обучить ИНС для восстановления блока открытого текста по доступному блоку шифртекста без восстановления ключа.

Еще одна новая актуальная проблема, связанная с ИНС и с машинным обучением, – **доверенный искусственный интеллект**.

4. Постквантовая криптография

Стойкость основных на сегодня асимметричных (с открытым ключом) криптографических платформ IFC (Integer Factorization Crypto, криптография на основе задачи факторизации), FFC (Finite Field Crypto, криптография в конечных полях), ECC (криптография на эллиптических кривых) основана на вычислительной сложности лежащих в их основе математических задач. На классическом компьютере эти задачи могут быть решены в лучшем случае за субэкспоненциальное время. Ситуация кардинально изменится, если будет построен промышленный квантовый компьютер. С его помощью целевые задачи можно будет **эффективно решить за полиномиальное время. Симметричная (с секретным ключом) криптография также окажется под ударом: фактическое сокращение примерно в два раза битовых длин ключей.**

Криптографическое сообщество активно прорабатывает **запасные криптографические платформы, которые сохраняют стойкость даже после «квантового апокалипсиса»**. Такие платформы принято называть постквантовыми. Основные из них: HBC (Hash-Based Crypto, криптография на основе функций хеширования), CBC (Code-Based Crypto, криптография на основе задач теории кодирования), LBC (Lattice-Based Crypto, криптография на основе теории решеток), MBC (Multivariate-polynomial-Based Crypto, криптография на основе многочленов от нескольких переменных).

В 2017 г. в США под эгидой Национального института стандартов и технологий (NIST) начался конкурс по разработке постквантовых алгоритмов и протоколов. В настоящий момент конкурс близится к завершению. В четвертый, заключительный, раунд вышли 5 систем платформы LBC (3 ШОК и 2 ЭЦП) и по одному представителю платформ CBC и MBC, т.е. LBC является безоговорочным лидером [17].

5. Проблемы совершенствования подготовки кадров в области информационной безопасности (ИБ)

- расширение перечня специальностей и их направлений для удовлетворения растущего спроса в кадрах по ИБ;
- привлечение специалистов-практиков для организации учебных, производственных, преддипломных практик и проведения учебных занятий в университетах с целью укрепления связи образования в области ИБ с практической деятельностью;
- формирование государственного кадрового заказа на специалистов по ИБ, особенно в интересах силовых министерств и комитетов, органов госуправления;
- привлечение организаций, являющихся потребителями выпускников-специалистов по ИБ, к укреплению материально-технической базы и финансированию научных исследований по ИБ в университетах;
- мониторинг использования специалистов по ИБ;
- согласование Перечней специальностей подготовки кадров высшей квалификации в РБ и РФ в области ИБ.

Литература

1. Математические и компьютерные основы криптологии. / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Мн.: Новое знание, 2003. – 413 с.
2. Молотков С. Квантовая криптография и теоремы В.А. Котельникова об одноразовых ключах и об отсчетах. / С. Молотков // Успехи физических наук. – 2006. – Т. 176, № 7. – С. 777–788.
3. Li Nianqiang Two approaches for ultrafast random bit generation based on the chaotic dynamics of a semiconductor laser. / N. Li, B. Kim, V.N. Chizhevsky, A. Locquet, M. Bloch, D.S. Citrin, W. Pan // Opt. Express. – 2014. – Vol. 22(6). – P. 6634–6646.
4. Пикуза М.О., Михневич С.Ю. Тестирование аппаратного генератора случайных чисел при помощи набора статистических тестов NIST. / М.О. Пикуза, С.Ю. Михневич // Доклады БГУИР. – 2021. – Т. 19 (6). – С. 37–42.
5. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2005. – 480 с.
6. Бережной И.Б., Харин Ю.С. Вероятностная модель динамики памяти криптографических генераторов Макларена – Марсальи. / И.Б. Бережной, Ю.С. Харин // Информатика. – 2014, № 1. – С. 105–115.
7. Brown, R. Dieharder: A Random Number Test Suite. – [Electronic resource]. http://www.phy.duke.edu/~rgb/General/rand_rate.php.
8. NIST SP 800-22: Download Documentation and Software. – [Electronic resource]. <https://csrc.nist.gov/projects/random-bit-generation/document-at-ion-and-software>.
9. Jones, G. Gjr and random numbers official site. – [Electronic resource]. <http://gjrandsourcesforge.net/>.
10. L'Ecuyer P. TestU01 – Empirical Testing of Random Number Generators. – [Electronic resource]. <http://simul.iro.umontreal.ca/testu01/tu01.html>.
11. Kowalska K.A. On the revision of NIST 800-22 Test Suites. – [Electronic resource]. <https://eprint.iacr.org/2022/540.pdf>.
12. Decision to Revise NIST SP 800-22 Rev. 1a. – [Electronic resource]. <https://csrc.nist.gov/news/2022/decision-to-revise-nist-sp-800-22-rev-1a>.
13. Программный комплекс для энтропийного анализа дискретных последовательностей. / В. Палуха, Ю. Харин, М. Мальцев [и др.] // Информационные системы

и технологии = Information Systems and Technologies: материалы междунар. науч. конгресса по информатике. – Т. 1. – 2022. – С. 102–107.

14. Палуха В.Ю., Харин Ю.С. Тестирование криптографических генераторов случайных и псевдослучайных последовательностей на основе энтропийных профилей. // Сб. конф. Комплексная защита информации. – Москва: Авангард. – 2022. – С. 117–122.

15. Волошко В.А., Трубей А.И. О мощности тестов многомерной дискретной равномерности, используемых для статистического анализа генераторов случайных последовательностей. / В.А. Волошко, А.И. Трубей // Журнал Белорусского государственного университета. Математика. Информатика. – 2022, № 1. – С. 26–37.

16. Alani M.M. Neuro-cryptanalysis of DES and triple-DES / M.M. Alani // Int. Conf. on Neural information processing. – N.Y.: Springer. – 2012. – P. 637–646.

17. Матвеев Г.В. Аналитический обзор методов и алгоритмов постквантовой криптографии. – Научно-технический отчет по НИР. – Минск: НИИ ППМИ БГУ, 2022. – 56 с.

РЕЗУЛЬТАТЫ РЕАЛИЗАЦИИ ПРОГРАММЫ СОЮЗНОГО ГОСУДАРСТВА В ОБЛАСТИ УКРЕПЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д.Н. АРЕСТОВИЧ, И.К. ЛЯШКО

*Научно-производственное республиканское унитарное предприятие
«Научно-исследовательский институт технической защиты информации»,
г. Минск, Республика Беларусь*

В рамках реализации Договора о создании Союзного государства отмечается дальнейшее развитие сотрудничества и интеграция Российской Федерации и Республики Беларусь в области обороны и безопасности, правоохранительной деятельности, военно-технического сотрудничества, таможенной, транспортной, энергетической, экономической, культурной и других сферах деятельности.

В соответствии с Программой действий Республики Беларусь и Российской Федерации по реализации Договора о создании Союзного государства в настоящее время выполняется комплекс мероприятий, в том числе предусматривающих:

- проведение единой торговой, налоговой, пограничной и таможенной политики;
- проведение совместной политики в области обороны, координацию деятельности в области военного строительства, совместного использования военной инфраструктуры;
- совместную деятельность правоохранительных органов и специальных служб;
- объединение энергетической и транспортной систем;
- формирование единой политики в области связи, объединение информационного пространства;
- осуществление совместной политики в области экологической безопасности, предупреждения и ликвидации последствий природных и техногенных катастроф;
- проведение единой политики в области стандартизации, метрологии и оценки соответствия.

Предупреждение и нейтрализация угроз безопасности информационным ресурсам в информационных системах Союзного государства и государств-участников могут быть обеспечены при условии согласованности применяемых Республикой Беларусь и Российской Федерацией требований, способов (методов) и средств защиты от угроз безопасности информации, что обуславливает необходимость осуществления совместной деятельности государств в области защиты информации.

В настоящее время завершена реализация программы Союзного государства «Совершенствование системы защиты информационных ресурсов Союзного государства и государств-участников Договора о создании Союзного государства в условиях нарастания угроз в информационной сфере» («Паритет») (далее – Программа), утвержденной Постановлением Совета Министров Союзного государства от 11 июня 2018 года № 5.

Целью Программы являлось усиление информационной безопасности Союзного государства и государств-участников в сфере защиты информационных ресурсов в информационных системах Союзного государства и государств-участников при их взаимодействии и совместном использовании в условиях нарастания информационных угроз, прогнозируемых на период до 2023 года.

Основными задачами, обеспечивающими достижение цели Программы, являлись:

создание научно-технических условий, необходимых для реализации мер по предупреждению и нейтрализации угроз безопасности информации в автоматизированных системах управления технологическими процессами критически важных объектов Республики Беларусь и Российской Федерации при их взаимодействии и совместном использовании (первая задача);

создание научно-технических условий, необходимых для реализации мер по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (государственные секреты), в информационных системах

Союзного государства и государств-участников при их взаимодействии и совместном использовании (вторая задача).

Исполнителями работ по мероприятиям Программы от белорусской стороны выступали государственные и негосударственные организации, в том числе научно-исследовательские, специфика деятельности которых связана с защитой информационных ресурсов. Весь предусмотренный Программой комплекс работ реализован в полном объеме и в установленные сроки.

Основными направлениями исследований, проводимых белорусской стороной в рамках реализации мероприятий Программы, являлись:

повышение устойчивости функционирования автоматизированных систем управления на критически важных объектах Республики Беларусь и Российской Федерации в условиях информационных угроз;

совершенствование оборудования для проведения специальных исследований технических средств защиты информации;

обеспечение эффективного мониторинга событий безопасности информационных систем с применением специального инструментария;

совершенствование инфраструктуры открытых ключей;

разработка программных и программно-аппаратных комплексов, направленных на обеспечение информационной безопасности.

В качестве основных направлений практического использования результатов реализации Программы можно отметить:

организацию производства в Беларуси и России разработанных в ходе выполнения Программы высокотехнологичных средств защиты информации;

обеспечение руководителей и специалистов, работающих в сфере обеспечения информационной безопасности Союзного государства и государств-участников, необходимыми нормативными и методическими документами, разработанными в ходе выполнения Программы;

применение полученных результатов в интересах Беларуси и России при разработке и введении в действие национальных нормативных и методических документов в области защиты информации.

Таким образом создание путем формирования и реализации мероприятий Программы совместных подходов к обеспечению безопасности государственных информационных ресурсов Союзного государства в условиях современных вызовов и угроз с учетом положений Концепции информационной безопасности Союзного государства создает единый фундамент для строительства согласованной государственной политики в информационной сфере Союзного государства.

ЭЛЕКТРОМАГНИТНЫЙ ТЕРРОРИЗМ КАК НОВЫЙ ВИД УГРОЗ ФУНКЦИОНАЛЬНОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

К.А. БОЧКОВ, Д.В. КОМНАТНЫЙ, И.О. ЖИГАЛИН

*Белорусский государственный университет транспорта,
г. Гомель, 246653, Республика Беларусь*

Проблема борьбы с терроризмом во всем мире с каждым годом становится все более актуальной. При этом терроризм со временем проникает в различные сферы жизнедеятельности людей и государств. Примерно два десятка лет назад появилось понятие электромагнитного терроризма, связанное с воздействием преднамеренных электромагнитных помех (ПЭМП) на микроэлектронные технические средства (МТС) информационно-телекоммуникационных автоматизированных систем, связанных с защитой информации и на МТС автоматизированных систем управления ответственными технологическими процессами (АСУ ОТП) на транспорте, энергетике, химических производствах. В обоих случаях эти системы относятся к критически важным объектам информатизации (КВОИ в Республике Беларусь) и критическим системам информационной инфраструктуры (КСИИ в Российской Федерации).

Под ПЭМП понимают преднамеренное оказание в преступных или террористических целях мощного электромагнитного воздействия на электронные и электрические системы, нарушающего их функционирование. Этот термин является дословным переводом общепринятого Международной электротехнической комиссией термина *Intentional Electromagnetic Interference* (IEMI). Воздействие ПЭМП на микроэлектронные системы возможно как по цепям питания, интерфейсным линиям, так и через свободное пространство.

Применительно к МТС информационно-телекоммуникационных автоматизированных систем ПЭМП рассматриваются как фактор угрозы информации в целях ее уничтожения, искажения или блокирования, т.е. относятся к предметной области информационной безопасности.

Воздействие ПЭМП на АСУ ОТП рассматривается как фактор угрозы нарушений условий безопасности функционирования в целях создания условий возникновения аварий, крушений, запредельных режимов работы и относятся к предметной области функциональной безопасности.

Наибольшую опасность для МТС информационно-телекоммуникационных систем (ИТС) и АСУ ОТП представляют малогабаритные переносные генераторы электромагнитных импульсов преднамеренного воздействия (ЭИПВ), излучающие энергию в диапазоне до 10 ГГц.

Существующие сегодня технологические возможности позволяют создавать излучатели электромагнитных импульсов (ЭМИ) с различными массогабаритными характеристиками [1] (от портативных до располагаемых на мобильной платформе), способные формировать с относительно больших расстояний (от единиц метров для портативных до нескольких сотен метров для мобильных источников) уровни падающих полей от 3 до 30 кВ/м, которые могут представлять опасность для микроэлектронных систем информационных инфраструктур. Воздействие таким малогабаритным генератором с близкого расстояния может вывести из строя до 20 компьютеров.

В отличие от проблемы электромагнитного терроризма классические вопросы электромагнитной совместимости (ЭМС) опираются на строгие, вполне определенные нормы и требования, заложенные в стандартах и используемые при испытаниях и измерениях. Современные микроэлектронные устройства АСУ ОТП (в том числе и в защищенном исполнении) и ИТС разрабатываются, проектируются и изготавливаются исходя из предъявляемых к ним требованиям стандартов по ЭМС. И если злоумышленники будут использовать генераторы ЭИПВ с характеристиками, превышающими уровни по помехозащищенности заложенные в соответствующих стандартах, то с большой вероятностью при воздействии (атаке) с помощью ЭИПВ это приведет к нарушению

функционирования микроэлектронных объектов защиты с различными последствиями нарушения их информационной и функциональной безопасности. Хотя многие из этих микроэлектронных систем АСУ ТП, ИТ-технологий спроектированы с учетом защиты от ударов молнии и ЭМ помех, заданных стандартами по ЭМС, однако они остаются уязвимыми к ЭИПВ из-за высокой импульсной мощности излучения и наличия разнообразных путей проникновения и наличия высокочувствительной быстродействующей элементной базы.

Основными причинами возрастания угрозы со стороны воздействия ЭИПВ (электромагнитного терроризма) являются:

1. Увеличение использования сложной и чувствительной электроники в системах обработки информации и управления критически важными компонентами инфраструктуры различных отраслей (энергетика, транспорт, связь, ответственные технологические процессы в промышленности и государственном управлении).

2. Эволюция микроэлектронных систем в направлении миниатюризации, увеличения плотности упаковки, повышения восприимчивости к электромагнитным помехам, увеличения количества портов, через которые проникают помехи и которые ранее не учитывались при разработке и производстве технических средств.

3. Увеличение количества коммерческих, весьма доступных источников ЭМ излучения, которые могут быть использованы в преступных целях.

4. В отличие от многих современных военных систем и автоматизированных систем в защищенном исполнении многие гражданские системы на основе использования компьютерных информационно-телекоммуникационных технологий не имеют охранных зон и специальных методов защиты от проникновения ЭИПВ.

5. Множество контуров в сложной микроэлектронной системе означает наличие множества резонансных частот, а спектр одиночного наносекундного импульса или пачки периодической последовательности импульсов имеют широкий спектр распределения энергии, перекрывающий тактовые частоты современных микроэлектронных систем.

Воздействие ЭИПВ на МТС ИТС и АСУ ОТП, как правило, приводит к нарушению требований по обеспечению как информационной, так и функциональной безопасности. При этом основные угрозы безопасности систем создаются за счет возможности уничтожения, искажения, блокирования информации или нарушения условий безопасности функционирования, приводящие к отказам в обслуживании или авариям, крушениям и нарушению условий обеспечения безопасности ответственных технологических процессов.

Особое место среди автоматизированных систем управления ответственными технологическими процессами занимают современные микроэлектронные системы железнодорожной автоматики и телемеханики (СЖАТ) призванные обеспечивать в первую очередь безопасность движения поездов. Это обусловлено предъявляемыми к ним техническими нормативно-правовыми актами (ТНПА), самыми высокими требованиями уровня полноты безопасности SIL4 по основополагающему международному и гармонизированному с ним межгосударственному стандарту ГОСТ МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью», состоящему из 7 частей [2].

Отличительной особенностью современных микроэлектронных систем обеспечения безопасности движения поездов (СЖАТ) является территориальная распределенность, расположение в городской среде (часто без определенного периметра охраны). При замене старых релейных СЖАТ на современные микроэлектронные, как правило в тех же зданиях и помещениях, уделяется мало внимания на обеспечение защиты от воздействия ЭИПВ по электромагнитному полю.

Поэтому разработка методов обеспечения защиты микроэлектронной аппаратуры СЖАТ к ЭИПВ, распространяющимся по свободному пространству, является актуальной научно-технической проблемой. Эти методы востребованы как на этапе разработки, так и на этапе сертификации СЖАТ. Подтверждением этому является реализация в Евросоюзе проекта «SECRET Security of railways against electromagnetic attacks» (Защита железнодорожных

систем от воздействия электромагнитных атак) [3], задачей которого является разработка превентивных мер по защите микроэлектронных и компьютерных СЖАТ от электромагнитных помех, в том числе и преднамеренного воздействия. В проекте задействовано десять организаций из пяти стран Евросоюза. Координатором является Французский институт науки и технологии транспорта (IFSTTAR). Однако в открытом доступе имеются лишь общие сведения по данному проекту.

Также в Евросоюзе реализован проект HIPOW Protection of Critical Infrastructures against High Power Microwave Threats (Защита критически важной инфраструктуры от угроз со стороны микроволнового излучения высокой мощности) [4]. Концепция HIPOW заключается в разработке новой нормативно-правовой и организационной базы для защиты от всех соответствующих электромагнитных угроз, которая включает методологии, процедуры и установленные обязанности, возможности для оценки рисков, тестирования, защиты и мер по обеспечению готовности к чрезвычайным ситуациям.

В США аналогичные исследования проводятся в рамках программы DEW (Directed Energy Weapons / направленное энергетическое оружие) Управления военно-морских исследований ONR (Office of Naval Research) [5]. Программа DEW была инициирована в ответ на быстрое развитие и растущую угрозу технологий направленной энергии.

Значительный опыт в НИЛ «Безопасность и ЭМС технических средств» БелГУТа, накопленный при испытаниях на ЭМС микроэлектронных СЖАТ в соответствии с установленными стандартами, позволяет рассматривать два подхода к решению проблемы защиты МТС от преднамеренных электромагнитных помех. Первый подход – физическое моделирование воздействия ЭИПВ на такие средства при помощи генераторов тестовых помеховых воздействий. Проведение таких экспериментов сталкивается со следующими трудностями. Во-первых, число помех и, соответственно, процедур испытаний, оказывается достаточно большим. Поэтому, возрастают сроки проведения испытаний. Во-вторых, генераторы-имитаторы ЭИПВ являются уникальными установками, как правило разрушающего действия, эксплуатация которых затрудняется необходимостью обеспечения безопасности прилегающих объектов. Поэтому в научно-технической литературе ставится задача комплексирования испытаний на электромагнитную совместимость микроэлектронного и компьютерного оборудования критически важных объектов информационной инфраструктуры к различным электромагнитным помехам. Эта же задача возникает в рамках проблемы анализа и прогнозирования стойкости микропроцессорной аппаратуры СЖАТ к ЭИПВ.

Существующей нормативно-технической документацией установлены испытания микроэлектронной аппаратуры СЖАТ на устойчивость к электростатическим разрядам (ЭСР) [6]. Используя принцип подобия, можно указать следующие сходные свойства ЭСР и ЭИПВ: длительность порядка единиц наносекунд и широкая полоса спектра; достаточная для создания сбоев и отказов энергия; воздействие на одни и те же каналы проникновения – неоднородности корпусов аппаратуры СЖАТ.

Допустимо считать, что паразитная антенна – неоднородность выделяет из фронта волны ЭИПВ импульс неизменной, по сравнению с импульсом на выходе генератора, формы с амплитудой, определяющейся условиями распространения. Иными словами, временные параметры импульса не изменяются [7]. Вся поглощаемая антенной мощность излучается внутрь корпуса аппаратуры СЖАТ. Такое предположение допустимо по принципу наихудших условий.

Если осуществить испытания микроэлектронной аппаратуры СЖАТ импульсом генератора-имитатора ЭСР с подобранными методом подобия параметрами, то по результатам испытания можно косвенно судить об устойчивости этих МТС к соответствующему ЭИПВ. Это обосновывается тем, что испытания осуществляются пропорционально-подобными импульсами. При этом появляется возможность исследовать наиболее интересующие проектировщика режимы воздействия ЭИПВ, спрогнозировать максимальную дальность поражения МТС источником ЭИПВ с его максимальной мощностью. Кроме того, одновременно можно установить устойчивость аппаратуры МТС СЖАТ к ЭСР. Согласно

действующим стандартам на ЭМС, использование такой процедуры испытаний, как минимум, исключает необходимость применения уникального испытательного оборудования, сокращает затраты средств, и, в меньшей степени, затраты времени на проведение сертификации СЖАТ по требованиям ЭМС.

Вторым подходом является математическое моделирование процесса проникновения ЭИПВ в корпуса аппаратуры микроэлектронных СЖАТ численными методами либо по аналитическим выражениям для электромагнитного излучения паразитных антенно-неоднородностей корпусов технических средств СЖАТ. Преимуществами этого подхода являются низкие затраты средств, универсальность используемых методов. Но недостатком этого подхода является то, что любая расчетная модель отражает процессы в реальном оборудовании всегда с некоторым приближением, связанным с ограничением математических моделей.

Применяя современные программные комплексы для численного моделирования, можно разработать 3D модель объекта испытаний (ОИ), учитывающую используемые в конструкции объекта материалы и параметры среды распространения. По этой модели производится расчет электромагнитных процессов в ОИ при воздействии ЭИПВ.

Численное моделирование позволяет учесть отражение и поглощение электромагнитных помех, что важно при сложной конструкции объекта испытаний. При моделировании воздействия наносекундных импульсных помех, в частности ЭСР и ЭИПВ, большое значение имеет возможность проследить пути распространения помехи внутри исследуемого объекта, учесть резонансы в корпусе аппаратуры. При подборе материала и конструкции ОИ можно сократить количество испытаний, предварительно промоделировав различные варианты их проведения. Также, появляется возможность предварительно проверить различные варианты защиты от воздействия широкополосных помех (геометрию расположения плат в корпусе и помехоподавляющих экранов).

Результат моделирования может быть наглядно представлен в виде диаграммы визуализации электромагнитного поля помехи либо в виде графиков (рис. 1).

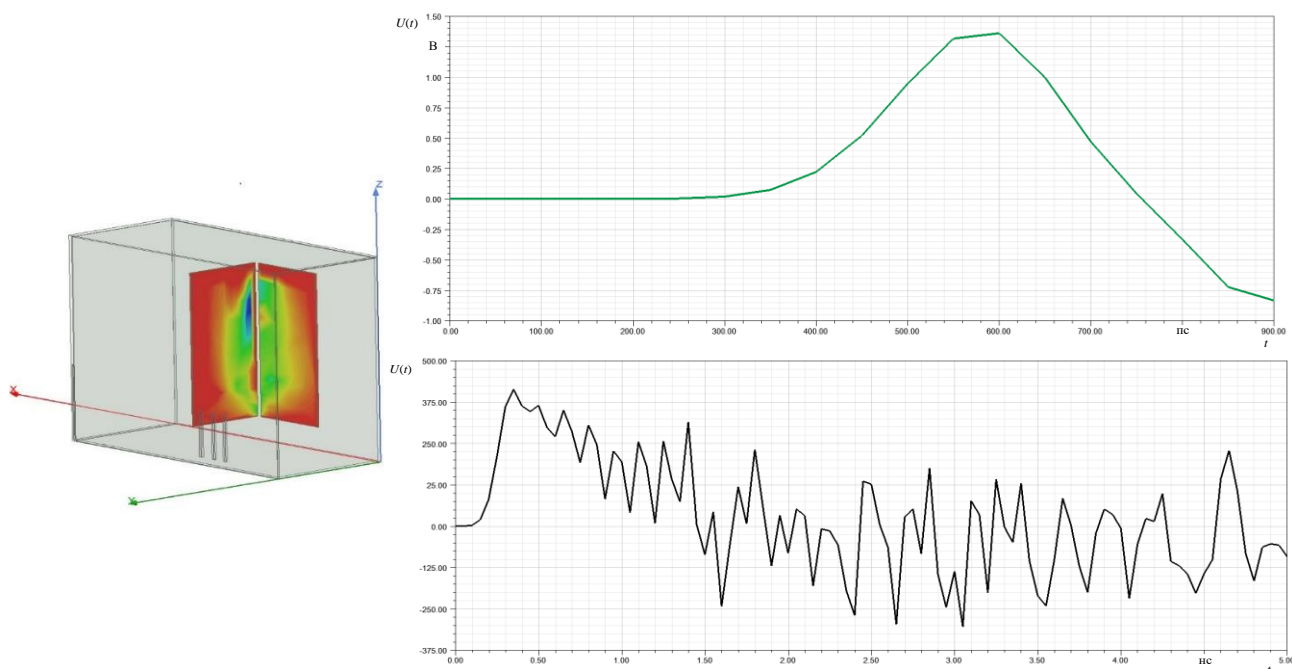


Рисунок 1. – Представление результатов моделирования

При оценке защищенности ОИ численное моделирование может дать гораздо больше информации чем аналитический расчет, но разработка компьютерной модели ОИ достаточно трудоемкий процесс. Вместе с тем, компьютерная модель, отражающая все особенности расположения узлов и элементов ОИ, оказывается настолько сложной, что начинают

проявляться ограничения численных методов и программно-аппаратного обеспечения. Эти ограничения и погрешности расчетов, а также влияние погрешностей задания исходных данных, не отражаются разработчиками доступных программных продуктов. Поэтому достоверность и адекватность результатов моделирования является неполной.

С другой стороны, аналитические модели отличаются более простым математическим аппаратом, вычислительной эффективностью, простотой реализации, отсутствием вычислительных трудностей. Таким образом, применение аналитических методов оправдано там, где требуется высокая скорость вычислений и быстрое получение результата, не в ущерб адекватности моделирования [8]. Наличие простых моделей и методов для расчета помех позволяет выполнить необходимые оценки на этапах проектирования и испытания МТС и принимать решения по оптимизации процедуры испытаний и повышению стойкости этих средств к ЭИПВ.

Прогнозирования воздействия ЭИПВ полезно при планировании процедуры натуральных испытаний, так как позволяет осуществить целенаправленную подготовку экспериментов, исключить влияние человеческого фактора, охватить испытанием наиболее опасные режимы воздействия ЭИПВ в пороговых областях.

Проводить численное моделирование целесообразно, если аппаратура СЖАТ на этапе разработки не прошла натурные испытания. В этом случае результаты моделирования применяются для поиска уязвимых мест. Для повышения помехоустойчивости потребуются проведение широкого комплекса расчетов большого числа вариантов конструкции аппаратуры СЖАТ, причем должна быть обеспечена высокая степень соответствия результатов расчетов и реально протекающих электромагнитных процессов. Аналитические методы на современном уровне развития обеспечивают только пессимистические оценки, т.е. с позиций наихудших условий, что гарантирует соответствие требованиям обеспечения УПБ/SIL 4 по ГОСТ Р МЭК 61508-2012 [2].

Заключение

1. В НИЛ «Безопасность и электромагнитная совместимость технических средств» Белорусского государственного университета транспорта разработаны аналитические методы расчета и прогнозирования поведения АСУ ОТП и, в частности, МТС СЖАТ при воздействии на них ЭИПВ. Исследования основаны на использовании принципа подобия при проведении стандартных методов испытаний 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. Необходимо дальнейшее развитие (исследование) методов анализа механизмов проникновения и прогнозирования последствий воздействия ЭИПВ через различные порты ТС современных микроэлектронных АСУ ТП в различных отраслях промышленности и информационных телекоммуникационных систем передачи, хранения и обработки информации.

4. Конечной целью таких исследований и внедрения их в практику защиты современных микроэлектронных систем в различных отраслях деятельности, связанных с обработкой, хранением и использованием информации в системах управления различного уровня, является минимизация последствий от влияния электромагнитных импульсов преднамеренного воздействия.

Литература

1. Белоконь И.Н., Гончаров А.Н., Долбня С.Н., Кудряшов А.С., Фотеев А.В. Оценка защищенности информационных инфраструктур от воздействия сверхкороткоимпульсных электромагнитных излучений техногенного происхождения. – Технологии электромагнитной совместимости. – 2010. – № 1. – С. 58–67.

2. ГОСТ Р МЭК 61508-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью.
3. SECRET – SECurity of the Railway network against Electromagnetic aTtacks, <http://www.secret-project.eu> (Дата доступа: 15.05.2023).
4. The HIPOW Project proposal. EU project grant nr. 284802.
5. Directed Energy Weapons: High Power Microwaves, <https://www.nre.navy.mil/organization/departments/aviation-force-projection-and-integrated-defense/aerospace-science-research-351/directed-energy-weapons-high-power-microwaves> (Дата доступа: 15.05.2023).
6. ГОСТ 30804.4.2-2013 (IEC 61000-4-2:2008) Совместимость технических средств электромагнитная. Устойчивость к электростатическим разрядам. Требования и методы испытаний.
8. Никольский, В. В. Теория электромагнитного поля / В. В. Никольский. – М.: Высшая школа, 1964. – 584 с.
7. Газизов, Т. Р. Уменьшение искажений электрических сигналов в межсоединениях / Т. Р. Газизов. – Томск: Изд-во НТЛ, 2003. – 167 с.

ЗАСЕДАНИЕ № 1

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

УДК 004.056:621.3

ОЦЕНКА ВОЗМОЖНОСТЕЙ ПЕРЕХВАТА ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ, ИСПОЛЬЗУЮЩИХ ЦИФРОВЫЕ ИНТЕРФЕЙСЫ

А.А. ХОРЕВ

Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Московский институт электронной техники», г. Зеленоград, Россия

Введение

Одним из наиболее опасных технических каналов утечки информации, обрабатываемой средствами вычислительной техники (СВТ), является канал утечки информации, возникающий вследствие побочных электромагнитных излучений (ПЭМИ) видеосистемы монитора.

В СВТ для передачи видеоданных широко используются цифровые интерфейсы DVI (Digital Visual Interface) и HDMI (High Definition Multimedia Interface), которые выполнены по стандарту последовательной передачи данных PanelLink с использованием технологии высокоскоростной передачи цифровых потоков TMDS.

При прохождении импульсных сигналов по видеокабелю вокруг последнего возникает побочное электромагнитное излучение (ПЭМИ).

Учитывая, что данные по интерфейсу TMDS передаются в последовательном виде, существует реальная возможность перехвата ПЭМИ и восстановления выводимого на экран монитора изображения.

Проведенные исследования показали, что если цвет пикселей изображения отличается, то и отличаются амплитуды «пиксельных» импульсов (группы импульсов, передающих цветовой код пикселя).

На рисунках 1 и 2 приведены спектры ПЭМИ видеосистемы с интерфейсом DVI при выводе на экран монитора тестовых изображений: белый экран и черный экран [1].

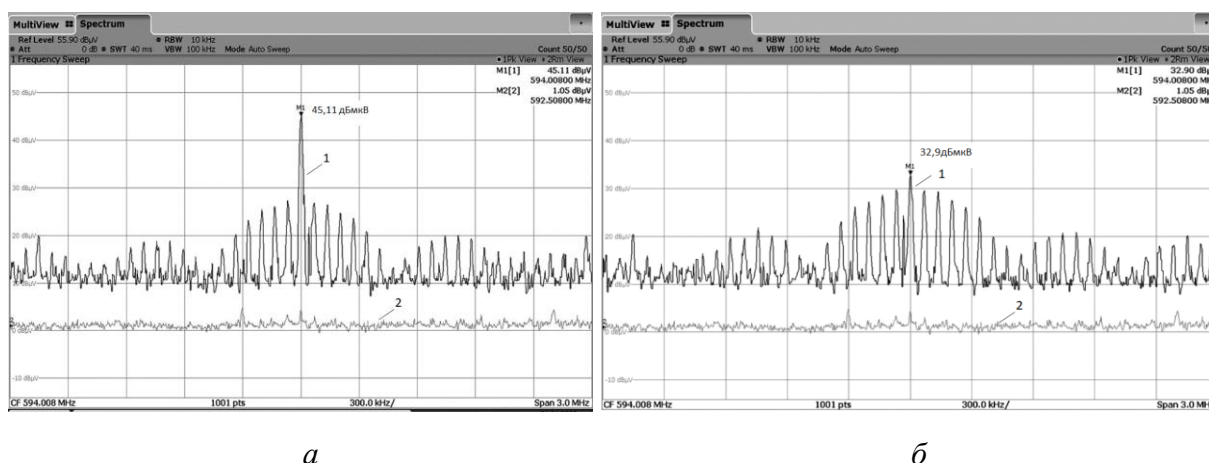


Рисунок 1. – Спектр ПЭМИ видеосистемы с интерфейсом DVI при выводе на экран монитора тестового изображения «белый» экран (а) и «черный» экран (б): 1 – спектр ПЭМИ; 2 – спектр шумов (видеосистема отключена)

1. Математическая модель перехвата побочных электромагнитных излучений средств вычислительной техники, использующих цифровые интерфейсы

Под математической моделью будем понимать совокупность уравнений и других математических соотношений, отражающих процесс перехвата ПЭМИ СВТ средством разведки.

Возможная упрощенная структурная схема средства перехвата ПЭМИ СВТ представлена на рисунке 2 [1].

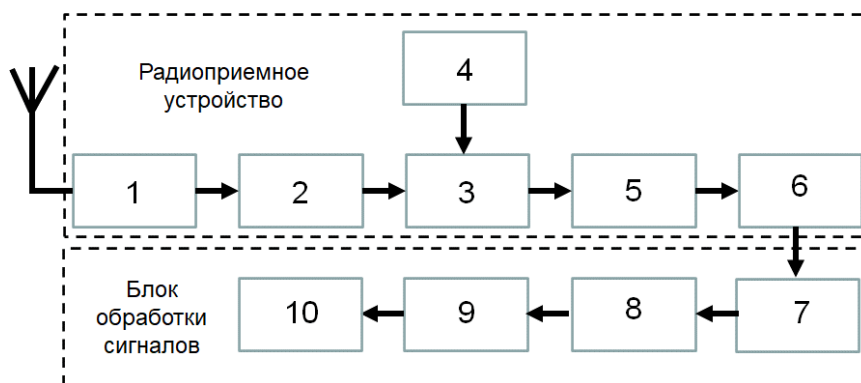


Рисунок 2. – Упрощенная структурная схема средства перехвата ПЭМИ СВТ:

- 1 – перестраиваемый полосовой фильтр высокой частоты; 2 – усилитель высокой частоты;
3 – смеситель; 4 – управляемый генератор (гетеродин); 5 – перестраиваемый полосовой
фильтр промежуточной частоты; 6 – усилитель промежуточной частоты; 7 – видеодетектор;
8 – аналого-цифровой преобразователь; 9 – блок цифровой обработки сигналов;
10 – ЖК-монитор

СВТ часто используются для обработки текстовых документов, содержащих сведения ограниченного доступа.

Возможность перехвата ПЭМИ видеосистемы с интерфейсом DVI и восстановления текстового изображения, выводимого на экран монитора, подтверждена экспериментально [2].

Известно, что разборчивость текста на зашумленном изображении зависит от отношения сигнал/шум изображения, при этом под сигналом обычно понимается разность средних яркостей белого и черного пикселей, а под шумом – среднеквадратическое отклонение яркости пикселей изображения, вызванное шумами приемника средства разведки [1, 2]:

$$q_c = 20 \lg \left[(L_b - L_c) / \sigma_{ш} \right] = 20 \lg (L_b - L_c) - 20 \lg (\sigma_{ш}), \quad (1)$$

где q_c – отношение сигнал/шум изображения, дБ;

L_b – средняя яркость белых пикселей, гр. ярк.;

L_c – средняя яркость черных пикселей, гр. ярк.;

$\sigma_{ш}$ – среднеквадратическое отклонение яркости пикселей изображения, вызванное шумами приемника средства разведки, гр. ярк.

При перехвате изображения, выводимого на экран монитора, необходимо учитывать, что оно стабильно в течение некоторого времени (T_a), которое зависит от характера действий оператора ПЭВМ и может варьировать от нескольких секунд (при наборе текста) до нескольких минут (при чтении текста). Данный факт позволяет использовать методы накопления (усреднения) кадров, что существенно повышает отношение сигнал/шум. Проведенные исследования показали, что накопление (усреднение) N изображений увеличивает отношение сигнал/шум в $k = \sqrt{N}$ раз [3].

С учетом накопления (усреднения) кадров формулу (1) запишем в виде будет равно:

$$q_{c.N} = q_c + 10\lg(N) = 20\lg(L_{\delta} - L_{\chi}) - 20\lg(\sigma_u) + 10\lg(N), \quad (2)$$

где q_c – отношение сигнал/шум изображения для одного кадра ($N = 1$), дБ;

$N = T_a \cdot F_k$ – количество кадров, перехваченных за время T_a ;

T_a – время, в течение которого изображение на экране монитора не меняется, с;

F_k – частота обновления экрана монитора, Гц.

Полагая, что яркость каждого пикселя перехваченного изображения прямо пропорциональна соответствующему напряжению на входе разведывательного приемника, и учитывая только шумы на входе приемного устройства средства разведки, с учетом накопления (усреднения) кадров отношение сигнал/шум изображения ($q_{c.N}$) можно рассчитать по формуле:

$$q_{c.N} = 20\lg(U_{\delta} - U_{\chi}) - 20\lg(\sigma_u) + 10\lg(N), \quad (3)$$

где U_{δ} – напряжение на входе приемного устройства средства разведки, соответствующие напряженности электрической (магнитной) составляющей побочного электромагнитного излучения (ПЭМИ), возникающего при передаче по интерфейсу импульсов белого цвета, мкВ;

U_{χ} – напряжение на входе приемного устройства средства разведки, соответствующие напряженности электрической (магнитной) составляющей ПЭМИ, возникающего при передаче по интерфейсу импульсов черного цвета, мкВ;

σ_u – среднеквадратическое отклонение напряжения шумов на входе приемного устройства средства разведки, мкВ.

Значения напряжений U_{δ} и U_{χ} определяются инструментально-расчетным методом, предполагающим для каждого частотного интервала измерение уровней напряженностей электрической (магнитной) составляющей электромагнитного излучения информативных составляющих ПЭМИ (E), расчета затухания ПЭМИ на трассе СВТ – средство разведки (V_r) и расчета U_{δ} и U_{χ} на входе приемного устройства с учетом калибровочных коэффициентов антенны средства разведки. Подробно данный метод описан в [1, 4, 5].

Учитывая, что роль случайных антенн при излучении ПЭМИ СВТ выполняют проводники, соединяющие выход цифроаналогового преобразователя видеоадаптера с разъемом DVI, и кабель, соединяющий системный блок с монитором, будем полагать, что в излучении ПЭМИ доминирует электрическая составляющая электромагнитного поля E_c , которая в ближней зоне убывает обратно пропорционально кубу расстояния ($\sim 1/r^3$), а дальней – обратно пропорционально расстоянию ($\sim 1/r$). Предположим, что в средней зоне электрическая составляющая электромагнитного поля E_c убывает обратно пропорционально квадрату расстояния ($\sim 1/r^2$). Границей начала дальней зоны будем полагать расстояние $r = 6\lambda$. Методика расчета затухания $V_{r.j.i}$ с учетом высказанных ранее допущений приведен в [1, 4].

Среднеквадратическое отклонение напряжения шумов на входе приемного устройства средства разведки в j -м частотном интервале зависит от уровня собственных шумов приемника ($\sigma_{u.n}$) и шумов антенны ($\sigma_{u.a}$) [1].

С учетом вышесказанного уравнение (3) можно записать в виде [1]:

$$q_{c.N.j} = 20 \lg \left[\sqrt{\sum_{i=1}^{N_j} (E_{\delta.j.i} / k_{a.j.i})^2} - \sqrt{\sum_{i=1}^{N_j} (E_{\psi.j.i} / k_{a.j.i})^2} \right] - 10 \lg \left[\frac{\sum_{i=1}^{M_j} (V_{r.j.i})^2}{M_j} \right] - 10 \lg \left[\frac{\Delta F_j \cdot Z \cdot \sum_{i=1}^{M_j} (N_{u.j.i})}{M_j} + \frac{\Delta F_j \cdot \sum_{i=1}^{N_j} (E_{ua.j.i} / k_{a.j.i})^2}{M_j} \right] + 10 \lg(N), \quad (4)$$

где $E_{\delta.j.i}$ – напряженность поля информативной составляющей ПЭМИ на i -й частоте, входящей в состав j -го частотного интервала (тест – «белый экран»), измеренная на расстоянии 1 м от СВТ, мкВ/м;

$E_{\psi.j.i}$ – напряженность поля информативной составляющей ПЭМИ на i -й частоте, входящей в состав j -го частотного интервала (тест – «черный экран»), измеренная на расстоянии 1 м от СВТ, мкВ/м;

$k_{a.j.i}$ – калибровочный коэффициент антенны средства разведки на i -й частоте, входящей в состав j -го частотного интервала, 1/м;

$V_{r.j.i}$ – затухание ПЭМИ на i -й частоте, входящей в состав j -го частотного интервала, в точке размещения средства разведки на расстоянии r ;

$N_{u.j.i}$ – спектральная плотность мощности собственных шумов приемника средства разведки, измеренная на i -й частоте при полосе пропускания $\Delta F = 1$ Гц и отношении сигнал/шум $q = 1$ в j -м частотном интервале, Вт/Гц;

ΔF_j – ширина j -го частотного интервала, Гц;

Z – входное сопротивление приемника средства разведки, Ом;

N_j – количество частотных составляющих в j -м частотном интервале;

M_j – количество частот, для которых проводится расчет в j -м частотном интервале.

2. Математическая модель оценки разборчивости перехваченного текста

Целью перехвата текстового изображения, выводимого на экран монитора, является получение смыслового содержания этого текста, поэтому в качестве показателя оценки возможности перехвата ПЭМИ СВТ техническим средством разведки (ТСР) используем словесную и фразовую разборчивость перехваченного текста.

Проведенные исследования показали, что разборчивость текста (W), выводимого на экран монитора, можно рассчитать по формуле [1, 3]:

$$W \approx \Phi(Q_1 \cdot q_c - Q_2), \quad (5)$$

где $\Phi(x) \approx \frac{1}{\sqrt{2\pi}} \cdot \int_{-\infty}^x \exp\left(-\frac{t^2}{2}\right) \cdot dt$ – интеграл вероятности;

q_c – отношение сигнал/шум изображения, дБ;

Q_1 и Q_2 – коэффициенты, зависящие от размера шрифта и особенностей восприятия оператором букв (цифр) на зашумленном изображении.

Значения Q_1 и Q_2 , определенные по результатам экспериментальных исследований, приведены в таблице 1 [1].

Таблица 1. – Значения коэффициентов Q_1 и Q_2 , определенные по результатам экспериментальных исследований

Показатель распознавания текста	Значение коэффициента Q_1	Значение коэффициента Q_2
Словесная разборчивость W_c	0,89	8,58
Фразовая разборчивость W_ϕ	1,65	14,74

Задаваясь пороговым (требуемым) значением разборчивости текста, из формулы (5) легко найти пороговое отношение сигнал/шум (δ):

$$\delta \approx [\Phi^{-1}(W_n) + Q_2] / Q_1, \quad (6)$$

где W_n – пороговое значение разборчивости текста;

$\Phi^{-1}(x)$ – функция, обратная $\Phi(x)$.

Учитывая, что словесная и фразовая разборчивости текста зависят от отношения сигнал/шум [1,3], можно установить критерии эффективности защиты текстовых документов, выводимых на экран монитора (см. таблицу 2). Пороговые значения δ_c и δ_ϕ приведены в [1].

Таблица 2. – Показатели и критерии эффективности защиты текстовой информации, при ее обработке СВТ

Цели защиты текстовых документов	Условия достижения цели защиты	Показатель эффективности защиты текстовых документов	Критерии эффективности защиты текстовых документов
Скрытие тематики текста	Количество правильно распознанных слов не позволяет установить тематику текста	Отношение информативный сигнал/шум на входе разведывательного приемника (q)	$q \leq \delta_c$
Скрытие содержания текста	Количество правильно распознанных фраз не позволяет составить аннотацию перехваченного текста	Отношение информативный сигнал/шум на входе разведывательного приемника (q)	$q \leq \delta_\phi$

3. Методика расчета опасной зоны R2

Для оценки возможностей средств разведки по перехвату ПЭМИ СВТ часто используют такое понятие, как опасная зона R2, под которой понимается пространство вокруг СВТ, в пределах которого отношение информативный сигнал/шум для ПЭМИ СВТ на входе разведывательного приемника (q) превышает допустимое (нормированное) значение (δ). То есть, это пространство вокруг СВТ, в пределах которого возможен перехват ПЭМИ и восстановление текста, выводимого на экран монитора, с требуемым для решения задач разведки качеством.

Расчет опасной зоны R2 осуществляется в следующей последовательности:

на основе измеренных значений спектральных составляющих ПЭМИ СВТ для расстояния $r = 1$ м ($V_r = 1$) для каждого j -го частотного интервала по формуле (4) рассчитываются отношения сигнал/шум ($q_{c.N.j}$) и сравниваются с пороговым значением (δ);

если для j -го частотного интервала $q_{c.N.j} > \delta$, то с шагом $\Delta r = 1$ м по формуле (4) рассчитываются отношения сигнал/шум ($q_{c.N.j}$) с учетом затухания ПЭМИ и сравниваются с пороговым значением δ . Для каждого частотного интервала расчет проводится до тех пор, пока $q_{c.N.j} \leq \delta$. Минимальные значения r_j , при которых выполняется условие $q_{c.N.j} \leq \delta$, фиксируются;

за значение R2 принимается максимальное значение из $\{r_j\}$ для всех частотных интервалов, то есть $R2 = \max\{r_j\}$.

Заключение

В качестве показателя оценки возможности перехвата текстовой информации, выводимой на экран монитора СВТ, средствами разведки ПЭМИ, целесообразно использовать

значение опасной зоны R_2 , зависящей от уровней ПЭМИ, затуханий ПЭМИ на трассе СВТ – средство разведки, уровней шумов на входе разведывательного приемника и порогового отношения сигнал/шум.

Предложен инструментально-расчетный метод расчета отношения сигнал/шум на входе разведывательного приемника с учетом измеренных уровней ПЭМИ на расстоянии 1 м от СВТ, рассчитанных затуханий ПЭМИ на трассе СВТ – средство разведки и рассчитанного значения уровней шумов на входе разведывательного приемника.

Предложен подход к расчету пороговых отношений сигнал/шум с учетом целей защиты текстовой информации: скрытие тематики текста и скрытие содержания текста.

Литература

1. Хорев А.А. Некоторые подходы к оценке возможностей перехвата побочных электромагнитных излучений средств вычислительной техники, использующих цифровые интерфейсы // Вестник УрФО «Безопасность в информационной сфере». – Челябинск, УрФО. – 2022. – № 3(45) – С. 5–16 ISSN: 2225-5435.

2. Хорев А.А., Феизов С.А. Экспериментальные исследования возможности перехвата текстовых изображений, выводимых на экран монитора // Международная конференция «Радиоэлектронные устройства и системы для инфотелекоммуникационных технологий – РЭУС-2020». Доклады. – М.: РНТОРЭС имени А.С. Попова, 2020. – С. 259–264. – URL: <https://elibrary.ru/item.asp?id=45676396> (дата обращения: 28.08.2022).

3. Хорев А.А. Методика оценки вероятности распознавания текстовых символов на зашумленных изображениях // Вестник УрФО «Безопасность в информационной сфере». – Челябинск, УрФО. – 2019. – № 4(34) – С. 5–14. – URL: <https://www.elibrary.ru/item.asp?id=41879982> (дата обращения: 28.08.2022).

4. Хорев А.А. Контроль защищенности средств вычислительной техники от утечки информации по техническим каналам. Часть 1 // Специальная техника. – М.: 2015. – № 1 – С. 53–63.

5. Хорев А.А. Контроль защищенности средств вычислительной техники от утечки информации по техническим каналам. Часть 2 // Специальная техника. – М.: 2015. – № 2 – С. 36–63.

ПРИНЦИПЫ ОБРАБОТКИ ДАННЫХ ОЦЕНКИ ЗАЩИЩЕННОСТИ КАНАЛОВ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ

В.К. ЖЕЛЕЗНЯК, А.Г. ФИЛИППОВИЧ,
К.Я.РАХАНОВ, М.М. БАРАНОВСКИЙ

*Учреждение образования «Полоцкий государственный университет
имени Евфросинии Полоцкой», г. Новополоцк, Республика Беларусь*

*Оперативно-аналитический центр при Президенте Республики Беларусь,
г. Минск, Республика Беларусь*

Введение

Техническая защита информации – это научное направление информатики, формирующее принципиально новые свойства защищенности объектов информатизации, информационных систем с дискретной формой представления сигналов, обработки результатов измерений с высокими точностными показателями параметров сигналов в виде периодической последовательности импульсов треугольной формы и сигналов шума квантования в виде периодической последовательности импульсов пилообразной формы с использованием современных микроэлектронных средств. Оптимальное управление снижает порог обнаружения широкополосной высококачественной образованной ступенчатой функцией с нелинейной амплитудной характеристикой аналоговых речевых сигналов (РС) в реальном масштабе времени. Сложность задач, решаемых информационными системами, разнообразие помеховых воздействий на сигналы обусловили общую проблему их защиты, оценку защищенности и контроля.

1. Основная часть

Частными задачами являются выбор помехоустойчивых измерительных сигналов (ИС) для передачи и оптимальной обработки принимаемых сигналов [1, 2]. Обработка ИС сводится к восстановлению полезной измерительной информации с наилучшими параметрами после обработки [2, 3, 4] в соответствии с принятым критерием. Оценка защищенности аналоговых и дискретно-квантованных РС должна выполняться по единому критерию. Идеальным квантующим устройством является ступенчатая функция [2]. Систематической ошибкой, присущей идеальной ступенчатой функции, является пилообразная функция с максимальным значением $\Delta/2$, среднеквадратическое значение $\sigma^2 = \Delta/\sqrt{12}$, плотность вероятности ошибки квантования составляет $1/\Delta$ [2].

В таблице 1 приведены значения дисперсии σ_e^2 в зависимости от шага квантования, из которого следуют весьма малые значения дисперсии для ее оценки в каналах утечки информации (КУИ) [1] по формуле $\sigma_e^2 = -(6,02b + 10,79)$ дБ. Здесь $\Delta = 2^{-b}$ – шаг квантования.

Таблица 1. – Значения дисперсии в зависимости от разрядности квантователя

Разрядность b , бит	8	10	12	14	16	18	20
Шаг квантования Δ	2–8	2–10	2–12	2–14	2–16	2–18	2–20
Дисперсия σ_e^2 , дБ	–59	–71	–83	–95	–107	–119	–131

Качественные улучшения метрологических и информационных характеристик процесса исследования основаны на определении точечных характеристик и параметров математических моделей [3].

Переход к оптимальным системам сводится к задаче оптимизации выбора структуры и параметров системы, при которой свойства последней оптимальны [4, 5]. Численные методы статистических испытаний реализуются с помощью средств вычислительной техники (СВТ) общего назначения с первичными измерительными преобразователями, программным обеспечением (ПО) в автоматизированном режиме. Обработку ИС выполняет оптимальный приемник [5, 6].

При проектировании и создании сложных информационных систем, в которых информационные потоки являются вероятностными, реализуют алгоритм ее функционирования, применяя метод имитационного моделирования, достоинством которого является возможность выполнения эффективных количественных и качественных исследований. Автоматизированные измерительные системы (СИА) реализовывают временные факторы в обработке большого объема данных измерений при других преимуществах в массогабаритных показателях, квантовании точности. Дискретно-квантованные преобразования обусловили возникновение новых КУИ, необходимость повышения чувствительности и точности выделения сигналов, прошедших четные и нечетные искажения.

Обработка результатов измерений в условиях слабых сигналов в шумах высокого уровня аналогичных и дискретно-квантованных РС выполняется с использованием закона больших чисел при выполнении ряда условий, получая новые качественные и количественные достоверные данные обработки [6, 7, 8]. Точечными значениями параметров находят действительные значения измеряемой величины при большом числе измерений. За действительные значения величины принимают точечную оценку истинного значения – среднее арифметическое значение при известном законе распределения результатов измерений [9].

Для оценки достоверности результатов измерений и ее увеличения пользуются доверительными интервалами и доверительными вероятностями. Доверительный интервал погрешности результата измерений – интервал значений случайной погрешности, внутри которой с заданной вероятностью находится истинное значение погрешности результата измерений [10]. Доверительные границы погрешности результата измерений – верхняя и нижняя границы доверительного интервала погрешности результата измерений [10]. Доверительные границы в случае нормального закона распределения вычисляются как $\pm tS$, где S – среднеквадратическая погрешность измерения, t – коэффициент, зависящий от доверительной вероятности P и числа измерений n [10].

Оценка истинного значения [8, 9] производится по данным выборки – ряда значений, принимаемых случайной величиной в процессе n независимых измерений. Основными параметрами функции распределения случайной величины X является математическое ожидание $M[X] = M_x$ и $D[X] = D_x$. Точечными оценками этих параметров (m_x^*, S_x) называются оценки, выражаемые одним числом. Чем больше выборка n , тем точнее определена функция нормального распределения измеряемой величины. Оценка истинного значения измеряемой величины определяется с помощью среднего арифметического значения $m_x^* = \bar{X}$ [6, 11], а с помощью статической дисперсии S_x^2 разброс измеряемой величины. Сигнал в КУИ (сигнал + шум) равен сумме $X(t)$ и $n(t)$. Маскирующий шум в КУИ подчиняется нормальному закону распределения.

Если даны значения X_1, X_2, \dots, X_n из n независимых опытов случайной величины X с неизвестным математическим ожиданием m_x (МО) M_x и дисперсией D_x , то для определения этих параметров следует пользоваться приближенными значениями. Несмещенной оценкой дисперсии является величина $D_x = S_x^2$ [9]. Вычисление среднеквадратического отклонения производится по следующей формуле [10]:

$$S_x = \sqrt{\sum_{i=1}^n (x_i - m_x^*)^2 / (n-1)}, \quad (1)$$

где x_i – результат i измерения величины X_i .

При увеличении числа независимых измерений n оценка среднего арифметического значения должна сходиться по вероятности к МО случайной величины. Такая оценка называется состоятельной и должна сходиться по вероятности к истинному значению величины при неограниченном увеличении независимых измерений n [9]:

$$\lim P(|m_x - m_x^*| < e), \quad (2)$$

где e – положительная величина;

P – доверительная вероятность.

Действительное значение физической величины [9] – значение физической величины, найденное экспериментальным путем и настолько близко к истинному значению, что для поставленной задачи может ее заменить. За действительное значение физической величины обычно применяется среднеарифметическое из ряда значений величин, полученных при равнооточных измерениях. Рассеивание результатов измерения – явление несовпадения результатов измерений одной и той же величины в ряду [10].

Среднеквадратическая погрешность единичного измерения (в ряду равнооточных измерений) S [10] – обобщенная характеристика рассеивания результатов, полученных в ряду независимых равнооточных измерений одной и той же физической величины вследствие влияния случайных погрешностей, вычисляемая по формуле:

$$S = \sqrt{\sum_{i=1}^n (x_i - \bar{X})^2 / (n-1)}, \quad (3)$$

Средняя арифметическая погрешность единичного измерения в ряду измерений [10] – обобщенная характеристика рассеивания n измерений, вычисляемая по формуле:

$$X = \sum_{i=1}^n |x_i - \bar{X}| / n, \quad (4)$$

где X – среднее арифметическое значение i погрешностей, присущих ряду измерений;

$|x_i - \bar{X}|$ – абсолютное значение погрешности измерения.

Среднеквадратическая погрешность результата измерений [10] – характеристика случайной погрешности среднего арифметического значения результата одной и той же величины в ряду измерений, вычисляемая как $S_x = S / \sqrt{n}$.

Точечная оценка при неизвестной дисперсии единичного измерения – оценивание с помощью: доверительных интервалов (метод Ю. Неймана). Наряду с выборочным средним \bar{X} вводится выборочная дисперсия [9] и ее несмещенная оценка:

$$S^2 = (1/(n-1)) \sum_{i=1}^n (x_i - \bar{X})^2. \quad (5)$$

Оценивание истинного значения производится по данным выборки. Основными параметрами функции распределения случайной величины являются МО и дисперсия.

Точечными оценками этих параметров называются оценки, выражаемые одним числом. Чем больше выборка и чем точнее определена функция распределения измеряемой величины, тем точнее с помощью среднего арифметического значения оценивается истинное значение измеряемой величины, а с помощью дисперсии – разброс измеряемых значений. В этом случае за действительные значения измеряемой величины принимают точечную оценку истинного значения – среднее арифметическое [9].

Используем математико-статистическую теорию ошибок, содержащую рациональные способы обработки результатов наблюдений и измерений, в основе которой одно из положений устанавливает принятие принципа арифметической середины, приводящей к тому, что измерения укладываются в нормальный закон распределения.

Ошибка измерения e представляет разность между результатом измерения величины X и истинным его значением $e = X - X_{ист}$ [12]. В широком классе задач точечная оценка действительных значений параметров определена. К недостатку оценивания относится несовпадение $X_{ист}$ с измеряемой величиной. Кроме того, необходимо знать дисперсию единичного измерения. Более совершенный способ оцениваний – способ доверительных интервалов [6, 9].

Доверительный интервал погрешности результата измерений – интервал значений случайной погрешности, внутри которого с заданной вероятностью находится искомое значение погрешности результата измерений. Доверительный интервал определяется зоной, равной $2tS_x$ для каждого измерения как среднего арифметического [9].

Доверительные границы погрешности результата измерений – верхняя и нижняя границы доверительного интервала погрешности результата измерений. Доверительные границы в случае нормального закона распределения вычисляются как $\pm tS$, где S – среднеквадратическая погрешность измерения; t – коэффициент, зависящий от доверительной вероятности P и числа измерений n [10].

Принимая точечную оценку $\bar{X} = m_x^*$ за истинное значение измеряемой величины $X_{ист}$ [11], необходимо определить ее точность. В качестве меры точности принимается интервал, определяемый доверительными границами $(-e, +e)$, в котором рассматривается ошибка оценки e , то есть истинное значение измеряемой величины с вероятностью $P_0 = 1 - q$ [6, 11] (q – уровень значимости) попадает в интервал $\bar{X} - e_x, \bar{X} + e_x$ [13]. Часто задают доверительный интервал от $\pm 3\sigma$, для которого доверительная вероятность составляет 0,9973.

Вводится переменная $t = e/\sigma$, функция $\Phi(t)$ является интегралом вероятностей и выражает вероятность попадания случайной величины t в интервале вероятности $P(-e \leq t \leq e) = 2\Phi(e)$. Значения функции приведены в таблице 2 [13].

Интервальные оценки используют с целью увеличения достоверности результатов измерений доверительными интервалами и доверительными вероятностями. Вероятность $\alpha = \Phi(t)$ называется доверительной вероятностью (табл. 3) [11].

Таблица 2. – Значения интеграла вероятностей $\Phi(e)$

e	$\Phi(e)$	e	$\Phi(e)$	e	$\Phi(e)$	e	$\Phi(e)$
0,00	0,000	0,70	0,516	1,40	0,839	2,25	0,976
0,10	0,080	0,80	0,576	1,50	0,866	2,50	0,988
0,20	0,159	0,90	0,632	1,60	0,890	2,75	0,994
0,30	0,236	1,00	0,683	1,70	0,911	3,00	0,9973
0,40	0,311	1,10	0,729	1,80	0,928	3,30	0,9990
0,50	0,383	1,20	0,770	1,90	0,943	3,50	0,9995
0,60	0,452	1,30	0,806	2,00	0,955	4,00	0,9999

Таблица 3. – Значения интеграла вероятностей $\Phi(t)$

$\Phi(t)$	$1 - \Phi(t)$	t	$\Phi(t)$	$1 - \Phi(t)$	t
0,50	0,50	0,675	0,992	0,008	2,652
0,60	0,40	0,842	0,993	0,007	2,697
0,70	0,30	1,036	0,994	0,006	2,748
0,75	0,25	1,150	0,995	0,005	2,807
0,80	0,20	1,282	0,996	0,004	2,878
0,85	0,15	1,440	0,997	0,003	2,968
0,90	0,10	1,645	0,998	0,002	3,090
0,95	0,05	1,960	0,999	0,001	3,291
0,96	0,04	2,054	0,9995	5×10^{-4}	3,481
0,97	0,03	2,170	0,9999	1×10^{-4}	3,891
0,98	0,02	2,326	0,9999	1×10^{-5}	4,417
0,99	0,01	2,576	0,9999	1×10^{-6}	4,892
0,991	0,009	2,612	0,9999	1×10^{-7}	5,327

Находят значение e , для которого выполняется равенство $\alpha = \Phi(t)$ [9]. При замене среднеарифметического значения истинным возникает погрешность $\pm e$ с вероятностью $\alpha = \Phi(t)$ того, что доверительный интервал с границами $(-e, +e)$ является истинным значением измеряемой величины. Чем шире доверительный интервал, тем выше вероятность попадания случайной погрешности измерений в этот интервал.

Принимая точечную оценку за истинное значение измеряемой величины, оценивают меру точности. В качестве меры точности рассматривают симметричный интервал $(-t, +t)$, в котором с заданной вероятностью располагается X_{ucm} . Вероятность попадания случайной погрешности в интервале, называемом доверительным интервалом с границами $\pm e$ при нормальном распределении, выражается функцией $\Phi(t)$ (табл. 2). Выражая границу e в значениях σ , находят $t = e/\sigma_m$ и $\Phi(t) = \Phi(t/\sigma_m)$, что соответствует доверительному интервалу $\pm e$ и называется доверительной вероятностью, а значение $1 - \Phi(t)$ – уровнем значимости. Значения функции $\Phi(t)$ и $1 - \Phi(t)$ приведены в таблице 3. На практике доверительная вероятность $\Phi(t)$ выбирается, в соответствии с таблицей 3, выше 0,9. Значение погрешности e , определяющей половину длины доверительного интервала $e = t(\sigma_x/\sqrt{n})$ [9]. Получаем, согласно [9]:

$$m_x^* - t(S_x/\sqrt{n}) \leq X_{ucm} \leq m_x^* + t(S_x/\sqrt{n}). \quad (6)$$

Абсолютная погрешность усредненных результатов измерений составляет $\Delta_n = \pm t(S_x/\sqrt{n})$ [9], где t определено по значению $\Phi(t)$ (табл. 3).

Доверительное значение погрешности измерения $\Delta = \pm t(S_n/\sqrt{n})$ [9]. Абсолютная погрешность усредненных результатов измерений $X_{ucm} = m_x^* \pm t(S_x/\sqrt{n})$ [9].

Заключение

Высокие требования к достоверности, точности результатов измерений обусловлены сложностью задач, решаемых информационными системами. Точечная и интервальная оценки значения параметров слабых сигналов в КУИ в условиях высоких уровней шумов снижают порог чувствительности, статистической обработкой – разброс измеренных значений, что

характеризует качество измерений и свойство измеряемой величины, доверительные интервалы и достоверные вероятности от конкретных условий достоверно устанавливать наличие (отсутствие) КУИ.

Литература

1. Гольденберг, Л.М. Цифровая обработка сигналов: справ. / Л.М. Гольденберг, Б.Д. Матюшкин, М.Н. Поляк. – М.: Радио и связь. 1986. – 312 с.
2. Бартон, Д. Справочник по радиолокационным измерениям / Д. Бартон, Г. Вард ; пер с англ. под ред. М.М. Вейсбейна. – М.,1976. – 392 с.
3. Вентцель, Е.С. Теория вероятностей / Е.С. Вентцель. – М.: Наука, 1984. – 576 с.
4. Тихонов, В.И. Оптимальный прием сигналов / В.И. Тихонов. – М.: Радио и связь, 1993. – 320 с.
5. Володарский, Е.Т. Планирование и организация измерительного эксперимента / Е.Т. Володарский, Б.Н. Малиновский, Ю.М. Туз. – Киев: Вища школа, 1997. – 280 с.
6. Линник, Ю.В. Метод наименьших квадратов и основы математико-статистической теории обработки наблюдений / Ю.В. Линник. – Изд. второе, испр. и доп. – Л.: Физматгиз, 1962. – 352 с.
7. Цыпкин, Я.З. Основы теории автоматических систем / Я.З. Цыпкин. – М.: Наука, 1977. – 560 с.
8. Левин, Б.Р. Теоретические основы статистической радиотехники / Б.Р. Левин. – М.: Сов. радио, 1968. – 584 с.
9. Кузнецов, В.А. Общая метрология / В.А. Кузнецов, Г.В. Ялунина. – М.: ИПК Изд-во стандартов, 2001. – 272 с.
10. Юдин, М.Я. Основные термины в области метрологии: слов.-справ. / М.Я. Юдин, М.Н. Селиванов, О.Ф. Тищенко, А.С. Скороходов ; под ред Ю.В. Гарбеева. – М.: Изд-во стандартов, 1989. – 113 с.
11. Тюрин, Н.Н. Введение в метрологию: учеб. пособие / Н.Н. Тюрин. – М.: Изд-во стандартов, 1989. – 248 с.
12. Венецкий, И.Г. Основные математико-статистические понятия и формы в экономическом анализе / И.Г. Венецкий, В.И. Венецкая. – М.: Статистика, 1974. – 279 с.
13. Электрорадиоизмерения: учеб. / В.И. Нефедов [и др.] ; под ред. проф. А.С. Сигова. – М.: Форум: Инфра, 2004. – 184 с.

МОДЕЛЬ УГРОЗ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ НА ВОЛОКОННО-ОПТИЧЕСКИХ ТЕХНОЛОГИЯХ

В.В. ГРИШАЧЕВ¹, А.Д. ЗАБОЛОТСКАЯ²

¹ *Российский государственный гуманитарный университет,
Институт информационных наук и технологий безопасности,
г. Москва, Россия*

² *Softline Company, г. Москва, Россия*

Введение

Совершенствование технологической базы информационных систем, телекоммуникационных сетей, автоматизированных систем управления приводит к созданию новых, ранее неизвестных угроз информационной безопасности. 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 в нормативных и методических документах.

Подобная проблема возникает с применением фотонных технологий в системах сбора, обработки, передачи и хранения 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 [1–5]

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 [1]. Наиболее перспективным абонентским доступом (первая/последняя миля) является оптический доступ в виде пассивных оптических сетей (*Passive Optical Network, PON*), который позволяет оптоволоконно 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 средам. Немаловажным 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 [2, 3]. 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 [4, 5]. 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, которые можно разделить на три направления:

- 1) угрозы перехвата трафика в оптических сетях различного назначения;
- 2) угрозы несанкционированного сбора информации на объектах через штатные оптические сети;
- 3) угрозы применения средств технической разведки 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 [6–11]

Перехват трафика – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов из информационных сетей (рис. 1). При перехвате объектом угрозы является информация, передаваемая по штатным оптическим сетям.

Оптическая кабельная система объекта может включать не только телекоммуникационные и локальные сети, но и сети специального назначения такие как аудиосвязи, 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 независимо 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 съема информации, т.е. нарушение конфиденциальности при передаче информации с помощью средств технической разведки. 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 [6–8].

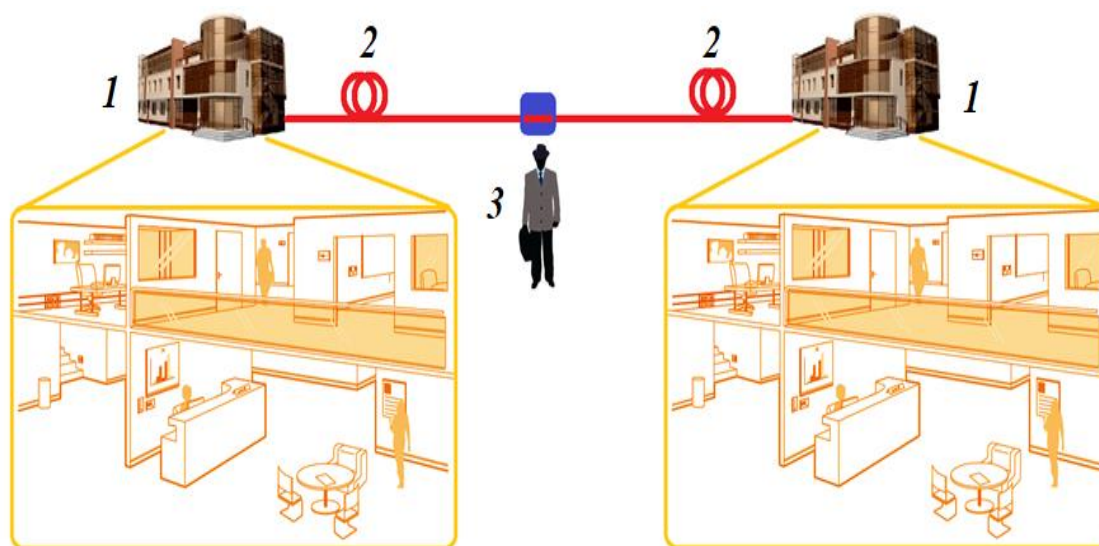


Рисунок 1. – Принципиальная схема перехвата трафика: защищаемые объекты (1), волоконно-оптическая линия связи (2), нарушитель со средствами технической разведки (3)

В структуре перехвата важную роль играют информативные сигналы и методы получения доступа к ним. В оптических сетях 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 оптоволокну с последующим отводом части оптического информационного сигнала путем установки специальной волоконно-оптической вставки в разрыв оптоволокну или путем воздействия на оптоволокну для вывода части оптического сигнала, например, на изгибе волокна, оптическом туннелировании и др. При дистанционном перехвате 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. Обсудим основные типы перехвата.

Модель угроз контактного перехвата трафика в оптических сетях

1. Контактный перехват с разрывом волокна

Наиболее простой и эффективный метод регистрировать информационный сигнал связан с использованием штатного устройства контроля за трафиком – волоконно-оптического перехватчика трафика (*Fiber Channel Traffic Access Point, TAP*), который может быть вставлен в штатный разрыв сети или подключен с помощью сварного соединения в созданный разрыв волокна. Вставка может быть реализована на основе оптических ответвителей.

2. Контактный перехват путем воздействия на волокно без разрыва [9]

Условие распространения оптического излучения в волокне определяется полным внутренним отражением на границе раздела сердцевина-оболочка, любые воздействия могут вызывать нарушение полного внутреннего отражения и появление побочных оптических излучений, выходящих из волокна. Наиболее просто это реализуется при механическом воздействии путем изгиба волокна. Устройства ввода/вывода на изгибе, например, волоконно-оптическая прищепка FOD-5503, используется при монтаже оптических сетей для аудиосвязи между монтажниками с помощью волоконно-оптических телефонов, не разрывая оптическую линию.

3. Контактный перехват на основе оптического туннелирования [10]

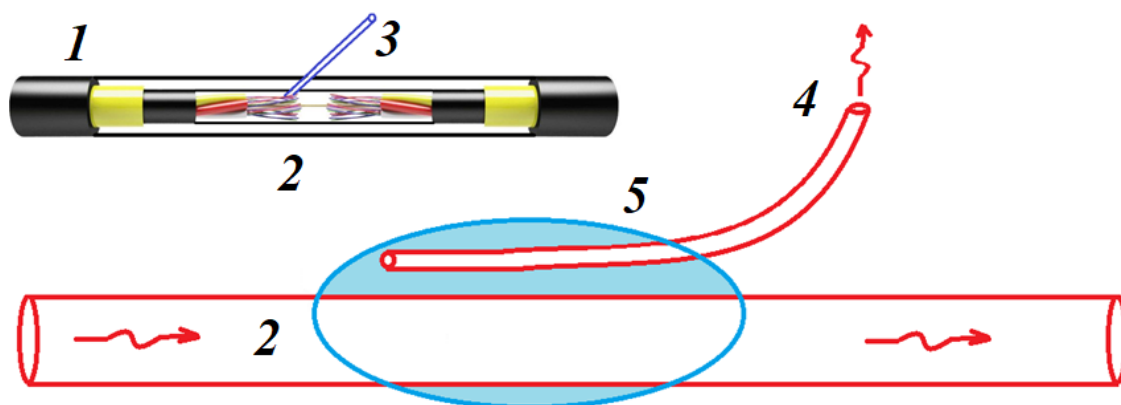


Рисунок 2. – Модель контактного перехвата на основе оптического туннелирования: оптический кабель с защитными оболочками (1), оптоволоконно канала связи (2), капиллярная трубка (3), оптоволоконно канала утечки (4), оптический клей (5)

Оптическое туннелирование состоит в переходе части оптического излучения из одного канала в другой близко расположенный отделенный оптическим слоем с меньшим показателем преломления, обеспечивающим полное внутреннее отражение. На данном явлении функционируют ответвители выполненные по технологии с боковым сплавлением волокон без пересечения оптических каналов. При перехвате данным методом, волокна каналов связи и утечки приводят в фиксированный оптический контакт, для чего не требуется значительных разрушений защитных оболочек кабеля и волокна. С помощью тонкой металлической трубки захватывается волокно канала связи, далее через трубку вводится оптический клей и волокно канала утечки, при затвердении клея формируется фиксированный оптический контакт между волокнами каналов связи и утечки (рис. 2).

Модель угроз дистанционного перехвата трафика в оптических сетях

1. Дистанционный перехват на основе вытекающих мод

Вытекающими модами называют выходящее из канала связи оптическое излучение при несогласованном соединении источника света и волокна, когда апертура источника превышает апертуру волокна. Вводимое в волокно оптическое излучение, выходящее за апертуру волокна, будет падать на границу раздела сердцевина-оболочка под углами меньшими критического и испытывать френелевское отражение с не нулевым преломлением. Эффект вытекающих мод может наблюдаться не только для входного информационного сигнала, но и по всей волоконно-оптической линии связи в местах подключения усилителей, повторителей, а также в местах дефектного соединения волокон или волокон с различающимися апертурами. Формирование дистанционного канала утечки возможно при наличии оптических окон в защитных оболочках кабеля или частичной оптической прозрачностью оболочек.

2. Дистанционный перехват на основе побочных оптических излучений

Побочным оптическим излучением можно назвать все локализованные по оптическому каналу связи излучения, вызванные рэлеевским рассеянием, френелевским отражением на оптических неоднородностях и др., которые могут выходить за пределы волокна и кабеля через оптические окна через защитные оболочки и слои кабельной системы (рис. 3).

В частности, побочные излучения могут формироваться при несогласованном сварном соединении волокон, т.е. когда волокна смещены друг относительно друга, сварены под углом друг к другу и др. Даже качественное соединение дает локализованные потери порядка 0,01 дБ, из которых некоторая часть захватывается волокном, а другая может выходить за пределы оболочек волокна. Сращенные волокна размещаются в кабельных муфтах подземной, подводной и воздушной проводки телекоммуникационных сетей, которые могут располагаться через каждые 3–5 км, что позволяет нарушителям выбрать наиболее подходящее место перехвата, при этом требуется наличие оптических окон в кабеле и муфте.

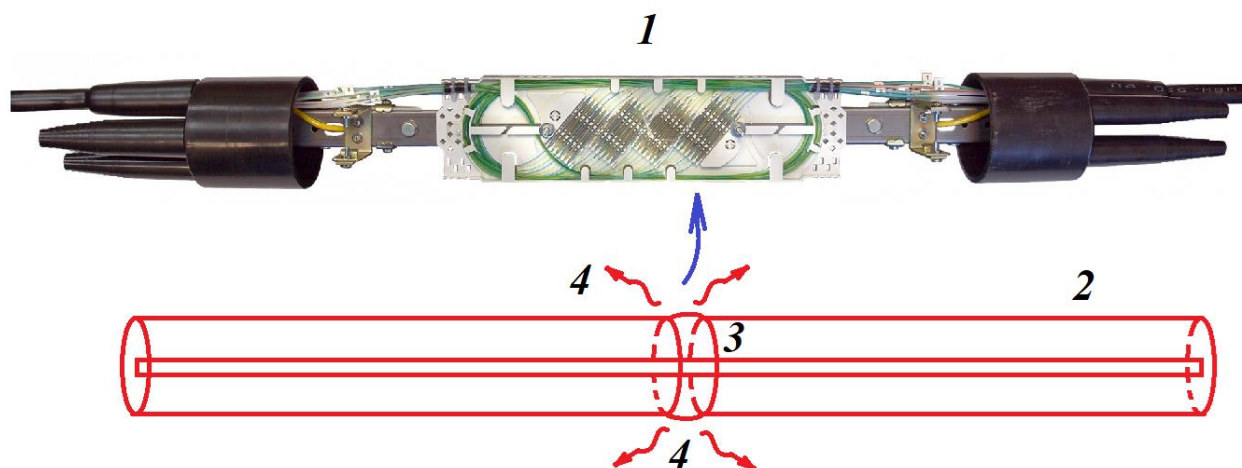


Рисунок 3. – Дистанционный перехват на основе побочных излучений: соединительная муфта (1), сращиваемое волокно (2), место сращивания волокон (3), побочное излучение (4)

1. Дистанционный перехват на основе паразитных электромагнитных излучений [11]

Паразитные электромагнитные излучения формируются в оптическом волокне вследствие нелинейно-оптических преобразований, приводящим к демодуляции информационного оптического сигнала на частотах близких к частоте модуляции оптической несущей, т.е. в миллиметровом и сантиметровом диапазоне длин волн, для которых диэлектрические защитные оболочки кабеля могут быть прозрачны. Мощность паразитных электромагнитных излучений определяется когерентностью прямого и величиной рассеянного информационного оптического потока.

2. Дистанционный перехват на основе параметрических методов

Параметрические методы регистрации информационного сигнала в оптическом канале связи вызываются модуляцией параметров волокна оптическим излучением информационного сигнала. Это может быть модуляция прецессии электронных или ядерных магнитных моментов, акустооптических эффектов, рентгеноструктурных эффектов и другое. В структуре параметрического перехвата используются внешние электромагнитные, рентгеновские, акустические поля, которые могут проходить защитные оболочки кабеля без его разрушения, что позволяет реализовать дистанционный перехват без прямой необходимости разрушения кабеля.

Оценим зону разведывательной доступности для дистанционного перехвата по побочным оптическим излучениям, как наиболее эффективным из описанных методов. Пусть побочное излучение формируется плоской неоднородностью в сердцевине волокна вследствие френелевского отражения величиной 30 дБ (т.е. 1/1000 от информационного сигнала), из-за дифракционной расходимости излучения ослабление составит 100 дБ на расстоянии 1 м от неоднородности размером порядка 10 мкм. Если другими потерями пренебречь, то в грубом приближении интенсивность информативного побочного оптического излучения составит 130 дБ от интенсивности информационного сигнала. Таким образом, зона разведывательной доступности не превысит цилиндр радиусом порядка 1 м с осью в виде кабеля. Поэтому выделение в модели угроз дистанционного перехвата можно считать условным, т.к. эффективный перехват возможен при прямом физическом контакте с оптическим кабелем.

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 на основе конвергенции функций передачи и измерения в штатных оптических сетях (рис. 4). В этом случае объектом угрозы является информация, циркулирующая на объекте вблизи оптических сетей в виде различного типа физических полей – речь, тепло, электромагнитные поля, радиационные поля и др.

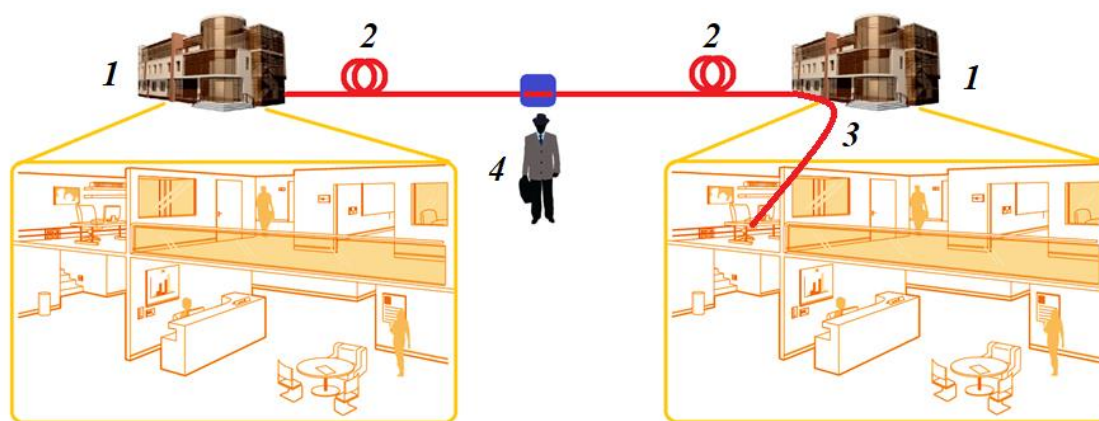


Рисунок 4. – Принципиальная схема несанкционированного сбора информации через штатные оптические сети: защищаемые объекты (1), волоконно-оптическая линия связи (2), локальная оптическая сеть (3), нарушитель со средствами технической разведки (4)

На объектах конфиденциальностью обладает не только внутренний и внешний трафик, но также и информация, циркулирующая внутри объекта в виде речи сотрудников, различных звуков работающего оборудования, электромагнитных полей, физических параметров окружающего пространства и т.д. Штатные волоконно-оптические коммуникации являются распределенной волоконно-оптической измерительной сетью с нештатными измерительными возможностями. Располагаясь внутри объекта, коммуникации проходят через или вблизи защищаемых помещений, в которых может свободно циркулировать конфиденциальная информация. Нарушитель может получить доступ к ней через 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 вследствие конвергенции транспортных и измерительных функций сети.

Обобщенная структура ТКУИ на основе волоконно-оптических коммуникаций объекта требует штатной/нештатной системы ввода/вывода зондирующего оптического излучения с формированием информативных сигналов утечки при воздействии на оптоволоконно-физического поля, связанного с конфиденциальной информацией. Воздействие вызывает модуляцию светового потока в оптоволоконке, которое переносит информацию за пределы контролируемой зоны, т.е. является информативным сигналом для модулирующего поля. Преобразующие возможности оптоволоконка определяют уровень опасности волоконно-оптического ТКУИ. В угрозе безопасности информации большую роль играет топология сети, так как прокладка оптического кабеля вблизи или через защищаемые помещения существенным образом влияет на защищенность от утечек.

Другие особенности связаны с возможностью использования для формирования информативного сигнала 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 вследствие варьирования параметров источника излучения. Сценарии по реализации ТКУИ через волоконно-оптические коммуникации могут быть различны в зависимости от возможности модуляции света в оптоволокну информативными полями и целей, преследуемых нарушителем.

Таким образом, в структуре волоконно-оптического ТКУИ выделяются основные направления реализации угроз – это методы зондирования штатной оптической сети, с помощью которой регистрируются информативные сигналы, и объекты оптической сети, на которых происходит модуляция зондирующего излучения. По методам и объектам зондирования можно построить модель угроз безопасности информации, циркулирующей на защищаемом объекте.

Модель угроз несанкционированного сбора информации через штатные оптические сети

1. Методы зондирования оптической сети

По существующей волоконно-оптической технике, используемой в несанкционированном сборе информации, можно выделить технику разведки:

– на прохождение, т.е. измерение параметров оптического излучения, прошедшего зондируемый объект, используемое для регистрации информативного сигнала на небольших расстояниях между источником и приемником, когда шумовые модуляции не превышают величины информативного сигнала;

– на отражение, т.е. оптическая рефлектометрия зондируемого объекта, используемое для регистрации информативного сигнала на максимальных расстояниях, определяемых техникой оптической рефлектометрии, так как позволяет выделить отклик от конкретного объекта зондирования;

Для зондирования на прохождение и отражение можно использовать все основные параметры оптического излучения и их комбинации – это модуляция интенсивности, фазы, частоты и поляризации, выбираемые исходя из эффективности (глубины) модуляции на объекте зондирования. В некоторых случаях для зондирования может применяться как оптическое излучение от средств технической разведки (нештатных источников), так и от штатных источников. В случае штатных источников и приемников, т.е. трансиверов оптической сети, зондирование обладает высокой скрытностью, но требует доступа к технике оптической сети (внутренний нарушитель).

Основой функционирования канала утечки является оптическая рефлектометрия [3], с помощью которой достигается возможность локализации отклика оптической сети наиболее чувствительной к воздействию информативных сигналов, проведения измерений одного информативного сигнала от нескольких объектов зондирования, повысить отношение сигнал/шум, проводить измерения в реальном времени и т.д. Развитие техники оптической рефлектометрии является одной из наиболее значимых угроз для несанкционированного сбора информации.

2. Объекты зондирования

Пассивные элементы оптической сети являются основными объектами зондирования, определяющие эффективность функционирования канала утечки, их можно разделить на:

– штатные пассивные элементы оптической сети, чувствительные к информативным физическим полям, – при изготовлении и монтаже оптической сети, как правило, не проводят исследований на возможный отклик пассивных оптических элементов на всевозможные внешние информативные физические поля, таким образом, у них могут существовать не декларируемые возможности не связанные с основными функциями в сети, например, конструкция разъемного соединения во многом совпадает с конструкцией волоконно-оптического микрофона с амплитудной модуляцией, но в декларируемых характеристиках разъемных соединителей акустические параметры не указываются;

– волоконно-оптические закладки, т.е. конструктивные изменения пассивных элементов оптической сети, внесенные с целью повышения чувствительности к окружающим информативным физическим полям, которые могут быть внесены в оптическую сеть;

3. Волоконно-оптические закладки

Конструктивные изменения пассивных элементов оптической сети могут быть произведены при изготовлении, при инсталляции, при эксплуатации оптической сети, каждая из которых имеет свои особенности и возможности, что позволяет произвести разделение угроз по трем направлениям:

– волоконно-оптические закладки производства – при производстве оптических элементов изготовитель может внести изменения в конструкцию пассивных элементов, которые не влияют на его функциональные возможности, но повышают чувствительность к внешним физическим полям.

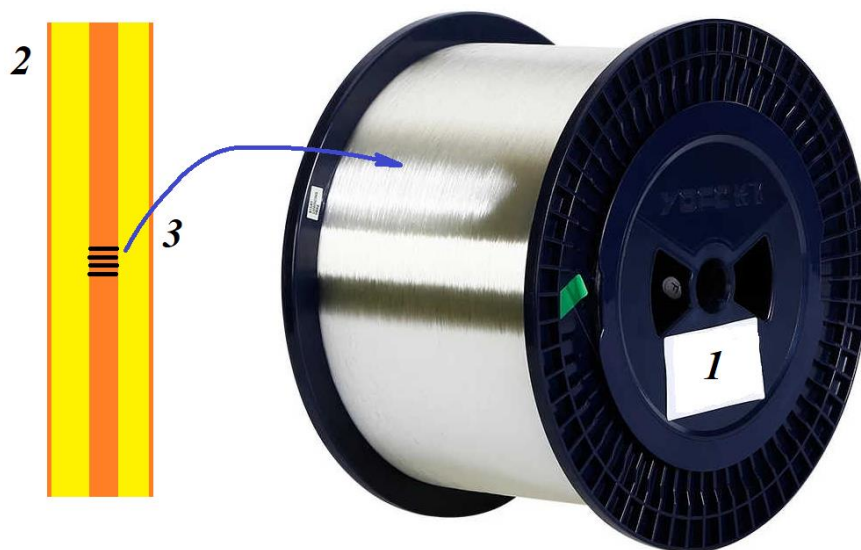


Рисунок 5. – Волоконно-оптическая закладка: катушка оптоволокна (1), элемент оптоволокна (2), решетка Брэгга (3)

Вносимые изменения могут относиться к оптическому волокну, к защитным оболочкам и другим элементам оптического кабеля. Одной из таких возможностей является создание брэгговских решеток в сердцевине волокна с длиной волны резонансного отражения на длинах волн в области поглощения материала волокна (рис. 5). Учитывая малую спектральную ширину резонансного отражения решетки, она не будет оказывать влияния на прохождение излучения на рабочих длинах волн канала связи в области окон прозрачности материала. Наличие таких решеток через каждые 100–200 м по длине кабеля создает возможность их расположения вблизи информативных сигналов при инсталляции кабельной системы. Таким образом, мониторинг оптической кабельной системы не позволит выявить такие волоконно-оптические закладки, так как мониторинг на длинах волн вне областей окон прозрачности не проводится на большие расстояния из-за большого поглощения. Если на длине волны 1550 нм поглощение в аморфном кварце уменьшается до 0,125 дБ/км, то на пиках поглощения 1383 нм превышает 1 дБ/км, а в видимой области поднимается выше 3 дБ/км.

Волоконно-оптическая закладка в виде брэгговской решетки позволяет создать высокочувствительный к акустическим, тепловым полям датчик информативных сигналов.

– волоконно-оптические закладки инсталляции – в процессе внутри объектного монтажа волоконно-оптической структурированной кабельной системы путем преднамеренного или непреднамеренного нарушения требований по выполнению работ могут быть изменена восприимчивость кабельной системы к внешним воздействиям, которые могут быть в том числе изначально не известны.



Рисунок 6. – Пример кабельного канала с пониженным акустическим контактом со стенами: гофротруба (1), пластиковая клипса (2)

Наиболее очевидные изменения могут связаны с нарушением нормативно-методических рекомендаций и требований, например, величина изгиба оптического кабеля превышает нормативные требования, проводка кабеля с натяжением, жесткое крепление кабеля к стенам и другое существенно повышают чувствительность к акустическим полям. С одной стороны, создаваемые отклонения могут быть не отмечены в требованиях к монтажу, так как не влияют на основную функцию кабельной системы – передавать информацию. С другой, их наличие еще не создает угроз безопасности информации, циркулирующей на объекте, если не учитывать расположение относительно защищаемых помещений.

Одним из таких отклонений, повышающих акустическую чувствительной кабельной системы, является место монтажа кабельных каналов. Жесткое крепление оптического кабеля к фундаментальным конструкциям здания, таким как железобетонные несущие стены, создают распределенную измерительную систему виброакустических колебаний в стенах – высокоинформативному структурному звуку, который слабо поглощается в монолитных строительных конструкциях. В качестве демонстрации снижения акустического контакта кабельного канала со стенами можно предложить использовать гофротрубу с креплением к стене с помощью клипсы, которые изготавливаются пластика с повышенной эластичностью (рис. 6). В таких кабельных каналах можно дополнительно провести акустическую изоляцию от стен (клипса) и внутри гофры, путем специальных звукопоглощающих прокладок.

– волоконно-оптические закладки эксплуатации – вносятся внутренним нарушителем путем локального механического, теплового, магнитного, электрического другого физического воздействия на кабельные каналы, оптический кабель структурированных кабельных систем защищаемого объекта на стадии эксплуатации оптической сети.

При функционировании волоконно-оптических подсистем структурированных кабельных систем объекта всегда есть возможность повысить эффективность несанкционированного сбора информации путем воздействия на нее. Вид воздействия зависит от задач и возможностей нарушителя, но основная цель такого воздействия – создать локальные оптические неоднородности кабельной системы вблизи защищаемого помещения, вблизи опасных элементов строительных конструкций. Например, угроза конфиденциальности переговоров может определяться не только близостью к защищаемому помещению, но и к акустическим волноводам в виде монолитных стен, воздухопроводов, водных

и другим хозяйственных коммуникаций здания. Соблюдение требований по нейтрализации угрозы на этапах инсталляции можно свести угрозы к минимуму, но внутренний нарушитель может механическим воздействием на кабельную систему, размещением источников полей вблизи нее в наиболее чувствительных местах вызвать повышение уровня угроз.

Модель угроз волоконно-оптического канала утечки речевой информации [12, 13]

Отдельным направлением технической разведки являются волоконно-оптический канал утечки акустической (речевой) информации, который определяется паразитной акустической модуляцией параметров светового потока в оптоволокне (рис. 7).

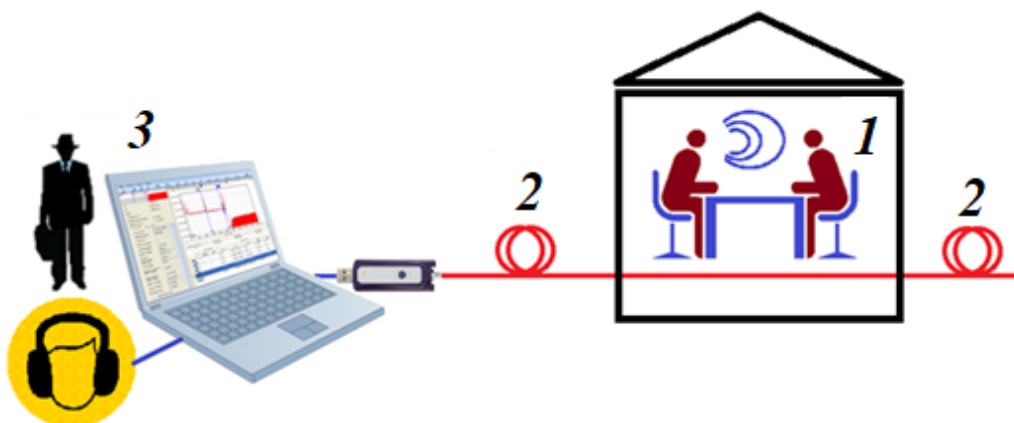


Рисунок 7. – Принципиальная структура канала утечки конфиденциальной речевой информации через волоконно-оптические коммуникации: защищаемое помещение (1), волоконно-оптическая линия связи (2), нарушитель со средствами технической разведки (3)

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 угрозу подслушивания конфиденциальных переговоров. Как показывают экспериментальные исследования, наибольшую опасность несут модуляции света на неоднородных участках оптического кабеля, связанные с виброакустическим воздействием (структурным звуком), а также возможность применения в качестве средств технической разведки стандартного волоконно-оптического оборудования, например, волоконно-оптического тестера-телефона с амплитудной модуляцией типа Рубин-021.

Реализация канала утечки речевой информации возможна методом нахождение оптического излучения или оптической рефлектометрии, путем использования параметров (интенсивности, фазы, поляризации и длины волны) штатного или нештатного оптического излучения. Фактически любой участок кабельной системы выступает источником информативных сигналов и использование оптической рефлектометрии позволяет создать распределенную волоконно-оптическую измерительную систему акустических колебаний.

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

Волоконно-оптические средства технической разведки – волоконно-оптические технические устройства (датчики), предназначенные для приема, регистрации и обработки информативных сигналов (рис. 8), при этом объектом угрозы является информация, циркулирующая на защищаемом объекте в виде различных физических полей – акустические, электромагнитные, оптические поля.

Преимущества волоконно-оптических технологий может быть использовано для создания волоконно-оптических средств технической разведки в виде волоконно-оптических датчиков и измерительных систем, адаптированных для выполнения специальных функций [2, 3]. 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 оптоволоком; обладают возможностью как точечных, так и распределенных измерений; не обнаруживаются стандартными электромагнитными способами, так как не содержат проводящих элементов; пассивны и нечувствительны к внешним электромагнитным полям; пожаробезопасны; миниатюрны и т.д. Все эти преимущества делают их очень эффективным средством технической разведки. В частности, волоконно-оптические микрофоны могут быть использованы в оперативной работе по скрытному подслушиванию переговоров.

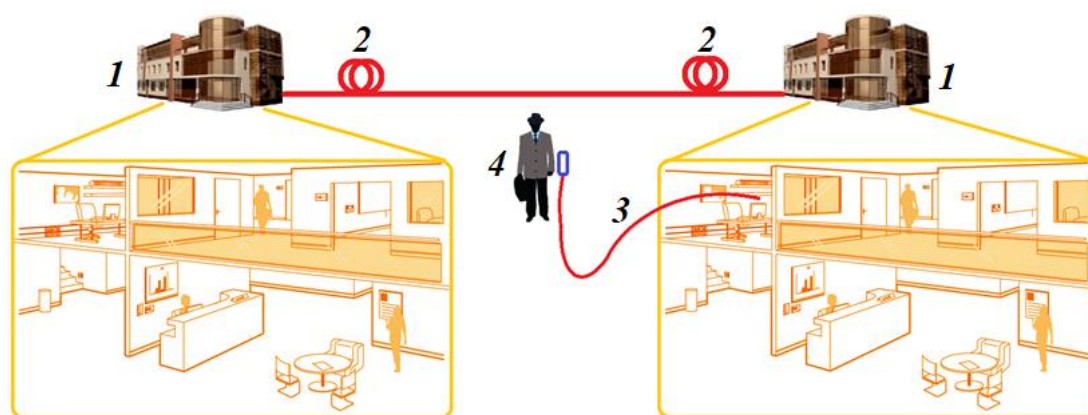


Рисунок 8. – Принципиальная схема применения волоконно-оптических средств технической разведки: защищаемые объекты (1), волоконно-оптическая линия связи (2), волоконно-оптические средства разведки (3), нарушитель со средствами технической разведки (4)

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 диффузном отражении от неподготовленной поверхности лазерного излучения или наоборот узкой направленности отраженного излучения 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 технической разведки требуют специальных исследований по обнаружению оптического волокна и кабеля, воздействию на его преобразовательные возможности для нейтрализации и др.

Заключение

Представленный анализ модели угроз информационной безопасности объектов с волоконно-оптическими технологиями показывает широкий спектр и высокий уровень возможных угроз, которые необходимо исследовать, разрабатывать возможные модели угроз, проводить обучение и переподготовку специалистов в данном направлении.

Литература

1. Складов О.К. Волоконно-оптические сети и системы связи – СПб.: Лань, 2010. – 272 с. ISBN 978-5-8114-1028-6
2. Волоконно-оптические системы мониторинга состояния инфраструктурных объектов / под ред. Дмитриева С.А. и Слепова Н.Н. – М.: Экслибрис-пресс, 2015. – 304 с. ISBN 978-5-88161-388-4
3. Листвин А.В., Листвин В.Н. Рефлектометрия оптических волокон – М.: ЛЕСАРарт, 2005. – 208 с. ISBN 5-902367-03-4
4. Гришачев В.В. Фотоника в системах безопасности и защиты информации. – Фотоника, 2011, № 6, с. 58–64.
5. Денисов В.И., Гришачев В.В., Косенко О.А. Волоконно-оптические технологии в системах безопасности и защиты информации. – Специальная техника, 2010, с. 47–61.
6. Зеневич А.О. Обнаружители утечки информации из оптического волокна: монография. – Минск: Белорусская государственная академия связи, 2017. – 142 с. ISBN 978-985-585-020-6
7. Шубин В.В. Информационная безопасность волоконно-оптических систем – Саров: РФЯЦ-ВНИИЭФ, 2015. – 257 с. ISBN 978-5-9515-0242-1
8. Алексеев Е.Б., Булавкин И.А., Попов А.Г., Попов В.И. Пассивные волоконно-оптические сети. Проектирование, оптимизация и обнаружение несанкционированного доступа / под ред. Е.Б. Алексеева – М: Медиа Паблишер, 2014. – 206 с. ISBN 978-5-903650-21-7
9. Гришачев В.В., Кабашкин В.Н., Фролов А.Д. Анализ каналов утечки информации в волоконно-оптических линиях связи: нарушение полного внутреннего отражения. – Информационное противодействие угрозам терроризма, 2005, № 4, с. 194–204. <http://www.contrterror.tsure.ru/>
10. Гришачев В.В. Перехвата трафика в оптических сетях: метод оптического туннелирования. – Фотоника, 2020. – Том 14, № 8. – с. 680–695. DOI: 10.22184/1993-7296.FRos.2020.14.8.680.695
11. Гришачев В.В. Перехвата трафика в оптических сетях: информативные паразитные электромагнитные излучения. – Фотоника, 2019. – Том 13, № 3. – с. 280–294. DOI: 10.22184/FRos.2019.13.3.280.294
12. Гришачев В.В., Казарин О.В., Калинина Ю.Д. Физическая модель угрозы утечки акустической (речевой) информации через волоконно-оптические коммуникации. – Вопросы защиты информации, 2018. – № 3. – с. 35–51.
13. Haiqing Hao, Zhongwang Pang, Guan Wang, and Bo Wang Indoor optical fiber eavesdropping approach and its avoidance. – Optical Express, 2022. – Vol. 30, Issue 20. – pp. 36774–36782. <https://doi.org/10.1364/OE.470529>.

ЗАЩИЩЕННОСТЬ ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ В ВОЛС

В.А. ДМИТРИЕВ, С.Н. КАСАНИН, Е.П. МАКСИМОВИЧ

*Государственное научное учреждение «Объединенный институт проблем
Информатики Национальной академии наук Беларуси»,
г. Минск, Республика Беларусь*

В настоящее время актуальной является проблема защиты информации, передаваемой по волоконно-оптическим линиям связи (ВОЛС).

В ВОЛС применяется, как правило, цифровая передача информации. Это обусловлено тем, что аналоговая передача информации требует высокой степени линейности промежуточных усилителей, которую трудно обеспечить в ВОЛС. Таким образом, наиболее распространенной ВОЛС является цифровая система с импульсно-кодовой модуляцией оптического излучения.

Самый простой и действенный способ защиты цифровой информации в ВОЛС – снижение мощности модулированного оптического излучения, которое может быть как одномодовым, так и многомодовым. Для обнаружения слабого модулированного оптического излучения используется метод счета фотонов [1], который является одним из наиболее чувствительных методов регистрации слабого модулированного оптического излучения.

Процесс передачи информационных сигналов осуществляется оптическими импульсами, распространяющимися вдоль ВОЛС [2], поэтому слабый оптический сигнал на выходе фотоприемника представляет собой последовательность флуктуирующих по амплитуде независимых «одноэлектронных» импульсов [3]. При этом статистика фотоэлектронов (фотоотчетов) повторяет статистику фотонов в плоскости чувствительного слоя фотоприемника [4].

Тип шума усилителя цифрового фотоприемника зависит от скорости передачи информации по ВОЛС. Когда скорость передачи информации по ВОЛС ≤ 500 Мбит/с, то преобладающими шумами усилителя цифрового фотоприемника являются дробовые шумы с пуассоновской статистикой, а для скоростей передачи информации по ВОЛС $C > 500$ Мбит/с, преобладающими шумами усилителя цифрового фотоприемника являются тепловые шумы с гауссовской статистикой [5].

При обнаружении информативных 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. Для обнаружения слабого модулированного оптического излучения необходимо использовать фотоприемник, работающий в режиме счета фотонов с последующим накоплением. В этом случае критерий Неймана-Пирсона соответствует условию, когда число отсчетов фиксировано. Для обнаружителя Неймана-Пирсона необходимо найти пороговое значение среднего числа фотонов, регистрируемых фотоприемником. Порог обнаружения (регистрации) выбирается, исходя из максимально допустимой вероятности ложной тревоги при данном среднем числе фотоэлектронов шума усилителя фотоприемника.

Оптимальным критерием обнаружения модулированного оптического излучения является отношение правдоподобия. Если модулирующим сигналом является цифровой информационный сигнал, то для последовательности независимых «одноэлектронных» импульсов логарифм отношения правдоподобия запишется следующим образом [6]:

$$d_{N,k} = \ln \left[\left(\frac{p_{c+\text{ш}}}{p_{\text{ш}}} \right)^k \cdot \left(\frac{1-p_{c+\text{ш}}}{1-p_{\text{ш}}} \right)^{N-k} \right] \geq D, \quad (1)$$

где N – число фотоотсчетов, равное числу импульсов модулированного оптического излучения;

k – число превышений некоторого уровня ограничений;

$p_{c+\text{ш}}$ – вероятность превышения уровня ограничения в случае, когда присутствует (сигнал + шум) (на выходе фотоприемника);

$p_{\text{ш}}$ – вероятность превышения уровня ограничения в случае, когда присутствует только шум (на выходе фотоприемника).

Из (1) получим минимальное значение k :

$$k \geq k_0 = E \left(\frac{A}{B} \right), \quad (2)$$

$$A = D - N \cdot \lg \left(\frac{1-p_{c+\text{ш}}}{1-p_{\text{ш}}} \right),$$

$$B = \lg \left[\frac{p_{c+\text{ш}}}{p_{\text{ш}}} \right] - \lg \left(\frac{1-p_{c+\text{ш}}}{1-p_{\text{ш}}} \right),$$

где $E(y)$ – целая часть y .

Если $k \geq k_0$, то принимается решение о наличии (сигнал + шум) на выходе фотоприемника. Если $k < k_0$, то принимается решение о наличии только шума на выходе фотоприемника.

1. Скорость передачи цифровой информации по ВОЛС $C \leq 500$ Мбит/с

$$p_{1,(c+\text{ш})} = \sum_{n=n_0}^{+\infty} \frac{(\overline{s_c} + \overline{s_{\text{ш}}})^n}{n!} \cdot \exp[-(\overline{s_c} + \overline{s_{\text{ш}}})], \quad (3)$$

$$p_{2,(c+\text{ш})} = \frac{1}{(1+\overline{s_c})} \cdot \exp\left(-\frac{\overline{s_{\text{ш}}}}{(1+\overline{s_c})}\right) \cdot \sum_{n=n_0}^{+\infty} \left(\frac{\overline{s_c}}{1+\overline{s_c}}\right)^n \cdot L_n \left[-\frac{\overline{s_{\text{ш}}}}{\overline{s_c} \cdot (1+\overline{s_c})}\right], \quad (4)$$

где $\overline{s_c} = \overline{I_c} \cdot T$ – среднее число сигнальных фотоэлектронов в плоскости чувствительного слоя фотоприемника, образованных за счет падающего на фотоприемник модулированного оптического излучения;

$\overline{s_{\text{ш}}} = \overline{I_{\text{ш}}} \cdot T$ – среднее число шумовых электронов в усилителе фотоприемника;

$\overline{I_c}$ – средний поток сигнальных фотоэлектронов;

$\overline{I_{\text{ш}}}$ – средний поток шумовых фотоэлектронов;

T – длительность выборки (время наблюдения);

n_0 – порог обнаружения модулированного оптического излучения;

$L_n(x)$ – полином Лагерра n -го порядка.

Выражение (3) справедливо в том случае, когда на фотоприемник падает одномодовое модулированное оптическое излучение, а выражение (4) справедливо в том случае, когда на фотоприемник падает многомодовое модулированное оптическое излучение.

2. Скорость передачи цифровой информации по ВОЛС $C > 500$ Мбит/с

$$p_{3,(c+\text{ш})} = \frac{1}{(1+\overline{s_{\text{ш}}})} \cdot \exp\left(-\frac{\overline{s_c}}{(1+\overline{s_{\text{ш}}})}\right) \cdot \sum_{n=n_0}^{+\infty} \left(\frac{\overline{s_{\text{ш}}}}{1+\overline{s_{\text{ш}}}}\right)^n \cdot L_n \left[-\frac{\overline{s_c}}{\overline{s_{\text{ш}}} \cdot (1+\overline{s_{\text{ш}}})}\right], \quad (5)$$

$$P_{4,(c+\text{ш})} = \frac{1}{(1+\bar{s}_c) \cdot (1+\bar{s}_\text{ш})} \cdot \sum_{n=n_0}^{+\infty} \left(\frac{\bar{s}_c}{1+\bar{s}_c} \right)^n \cdot \left[1 + \frac{q \cdot (q^n - 1)}{1+q} \right]. \quad (6)$$

Выражение (5) справедливо в том случае, когда на фотоприемник падает одномодовое модулированное оптическое излучение, а выражение (6) справедливо в том случае, когда на фотоприемник падает многомодовое модулированное оптическое излучение.

Вероятность обнаружения модулированного оптического излучения и вероятность ложной тревоги определяются следующим образом:

$$P_{\text{обн.}} = \sum_{k=k_0}^N C_N^k \cdot p_c^k \cdot (1-p_c)^{N-k} = B_{p_c}(k_0, N - k_0 + 1), \quad (7)$$

$$P_{\text{лт}} = \sum_{k=k_0}^N C_N^k \cdot p_\text{ш}^k \cdot (1-p_\text{ш})^{N-k} = B_{p_\text{ш}}(k_0, N - k_0 + 1), \quad (8)$$

$$B_x(a, d) = \int_0^x \frac{\Gamma(a+d)}{\Gamma(a)\Gamma(d)} \cdot x^{a-1} \cdot (1-x)^{d-1} dx, \quad (9)$$

где $B_x(a, d)$ – неполная бета-функция;

$\Gamma(g)$ – гамма-функция.

При больших N вероятность обнаружения модулированного оптического излучения и вероятность ложной тревоги определяются следующим образом:

$$P_{\text{обн.}} \approx 1 - \Phi \left[\frac{k_0 - N \cdot p_c}{\sqrt{N \cdot p_c \cdot (1-p_c)}} \right], \quad (10)$$

$$P_{\text{лт}} \approx 1 - \Phi \left[\frac{k_0 - N \cdot p_\text{ш}}{\sqrt{N \cdot p_\text{ш} \cdot (1-p_\text{ш})}} \right], \quad (11)$$

где $\Phi(t) = \frac{1}{\sqrt{2\pi}} \cdot \int_{-\infty}^t \exp\left(-\frac{y^2}{2}\right) dy$ – интеграл вероятности.

Полное скрытие информации в ВОЛС достигается только в том случае, когда $P_{\text{обн.}} \leq 0,3$ [7].

Литература

1. Ветохин С.С. Одноэлектронные фотоприемники / С.С. Ветохин, И.Р. Гулаков, А.Н. Перцев. – М.: Энергоатомиздат, 1986. – 246 с.
2. Наний О.Е. Приемники цифровых волоконно-оптических систем связи / О.Е. Наний // Lightwave Russian Edition. – 2004. – № 1. – С. 50–51.
3. Матвеев И.Н. Лазерная локация / И.Н.Матвеев, В.В.Протопопов, И.Н.Троицкий, Н.Д.Устинов; под ред. Н.Д.Устинова. – М.: Машиностроение, 1984. – 272 с.
4. Гудмен Дж. Статистическая оптика / Дж. Гудмен. – М.: Мир, 1988. – 528 с.
5. Шубин В.В. Информационная безопасность волоконно-оптических систем / В.В.Шубин. – Саратов: РФЯЦ-ВНИИЭФ, 2015. – 257 с.
6. Ключев Н.Ф. Обнаружение импульсных сигналов с помощью накопителей дискретного действия / Н.Ф.Ключев. – М.: Изд-во «Советское радио», 1963. – 113 с.
7. Хорев А.А. Оценка эффективности защиты информации от утечки по техническим каналам / А.А. Хорев // Специальная техника. – 2006. – № 6. – 53–61

МЕТОДЫ РАСЧЕТА ПОМЕХОВОГО ЭЛЕКТРОМАГНИТНОГО ПОЛЯ, ПРОНИКАЮЩЕГО ЧЕРЕЗ КРУГЛОЕ ОТВЕРСТИЕ В ПЛОСКОМ ЭКРАНЕ

Д.В. КОМНАТНЫЙ

*Белорусский государственный университет транспорта,
г. Гомель, Республика Беларусь*

Составной частью проблемы комплексной защиты информации является защита критически важных объектов информационной инфраструктуры от воздействия некондуктивных электромагнитных помех. Особенную актуальность этот вопрос приобретает в современных условиях, когда имеется возможность осуществления деструктивных воздействий на указанные объекты с помощью преднамеренных электромагнитных помех (электромагнитный терроризм). Целью воздействия указанных помех могут оказаться оборудование хранения больших объемов информации (серверы), оборудование сетей передачи данных, оборудование конечных пользователей. В частности, потенциальным объектом воздействия оказываются диспетчерские центры магистральных железных дорог и высокоскоростных городских линий, а также современные микропроцессорные системы управления движением поездов.

Основным средством защиты от некондуктивных помех является электромагнитное экранирование. Вопросы проектирования сплошных электромагнитных экранов хорошо разработаны [1, 2]. Но практическое изготовление сплошных экранирующих оболочек затруднено необходимостью наличия различных технологических отверстий в экране. Поэтому необходимы средства анализа проникновения помехового электромагнитного поля через отверстия в экране.

Л.И. Мандельштам и Х. Бете предложили способы расчета проникновения электромагнитного поля через круглое отверстие в бесконечном металлическом экране [3, 4]. Способ Х. Бете базируется на рассмотрении более простой задачи о проникновении через такое отверстие электростатического или магнитостатического поля. Поэтому для инженерных целей необходим простой и эффективный способ решения последней задачи.

В литературных источниках предложено большое число решений задачи о проникновении равномерного электростатического поля через круглое отверстие в проводящем плоском экране. Эти решения отличаются выбором системы координат для описания электродинамической системы задачи. Разнообразие теоретических решений затрудняет их приложение к практическим расчетам конструкций электромагнитных экранов. Поэтому в докладе предпринята систематизация опубликованных результатов и их отбора по критерию вычислительной эффективности для практических приложений.

В [1] для решения рассматриваемой задачи применена сферическая система координат с центром, совпадающим с центром отверстия. Вводится сфера радиуса, равного радиусу отверстия. На поверхности сферы требуется удовлетворение граничным условиям непрерывности векторов нормальной и тангенциальной составляющих вектора напряженности электростатического поля. Это позволяет получить выражения для потенциала поля в области отверстия, в областях до экрана и за экраном.

Так, выражение потенциала поля в области за экраном имеет вид

$$u_2 = -\sin \varphi \sum_{n=2k}^{\infty} C_n r^{-n-1} P_n^1(\cos \theta) \sin \varphi ,$$

где u_2 – потенциал, В; θ , φ – угловые сферические координаты, рад; C_n – постоянные интегрирования, В; r – радиальная сферическая координата, м; P_n – полином Лежандра.

Недостатками такого решения являются: введение сферической поверхности, не заданной физическими соображениями; представление решения в форме бесконечного ряда. Последнее вызывает необходимость оценки числа удерживаемых членов ряда и усложняет расчет с требуемой точностью.

Решение в цилиндрической системе координат требует выполнения граничного условия равенства нулю потенциала экрана и условия сопряжения на отверстии. Условие сопряжения заключается в том, что напряженность поля в отверстии численно равна напряженности поля, которая существовала бы на поверхности сплошного экрана, и имеет только нормальную составляющую. Тогда потенциал в области за экраном имеет выражение [5]

$$u_2(r, z) = \int_0^{\infty} C(\lambda) e^{-\lambda z} J_0(\lambda r) d\lambda,$$

где $C(\lambda)$ – функция; λ – расчетная переменная; z, r – линейные цилиндрические координаты, м; J_0 – функция Бесселя первого рода нулевого порядка.

В [5] показано, что для функции $C(\lambda)$ справедливо парное интегральное уравнение

$$\int_0^{\infty} \lambda C(\lambda) J_0(\lambda r) d\lambda = E_0 \quad 0 \leq r \leq a,$$

$$\int_0^{\infty} C(\lambda) J_0(\lambda r) d\lambda = 0 \quad a < r \leq \infty,$$

где a – радиус отверстия, м; E_0 – напряженность электростатического поля в области до экрана, В/м.

Там же показано, что решение этого парного интегрального уравнения имеет замкнутую математическую форму, таким образом, функция $C(\lambda)$ равна

$$C(\lambda) = \frac{2}{\pi} \int_0^a \sin \lambda t dt \int_0^t \frac{y E_0}{\sqrt{t^2 - y^2}} dy = \frac{2 E_0}{\pi} \left[\frac{1}{\lambda^2} \sin \lambda a - \frac{a}{\lambda} \cos \lambda a \right].$$

Недостатком этого решения является необходимость вычислять несобственный интеграл от специальной функции Бесселя, что затрудняет инженерные расчеты.

В [3, 6] получено решение рассматриваемой задачи в эллипсоидальной системе координат. В этой системе координат потенциал поля в области за экраном имеет замкнутое выражение

$$u_2(x, z) = \frac{E_0 z}{\pi} \left(\operatorname{arctg} \lambda + \frac{1}{\lambda} \right),$$

$$\lambda = \sqrt{\frac{1}{2} \left(\frac{z^2}{r_0^2} + \frac{x^2}{r_0^2} - 1 \right) + \frac{1}{2} \sqrt{4z^2 + \left(\frac{z^2}{r_0^2} + \frac{x^2}{r_0^2} - 1 \right)^2}},$$

где x, z – декартовы координаты, м; r_0 – радиус отверстия, м.

Достоинством приведенного решения является то, что оно имеет замкнутую форму и не использует бесконечных рядов или несобственных интегралов.

Проведенный в докладе сравнительный анализ предложенных решений задачи о проникновении электростатического поля через круглые отверстия в плоском экране показывает, что наиболее удобным для практического использования является решение, представленное в эллипсоидальных координатах. Как видно, оно имеет меньше источников возможных расчетных ошибок и погрешностей решения. Эллипсоидальная координата λ

достаточно просто выражается через декартовы, поэтому применение эллипсоидальной системы координат не вызывает затруднений при анализе реальных конструкций экранов и корпусов. Эллипсоидальную координату можно рассматривать как параметр, не учитывая ее геометрический смысл.

На больших расстояниях от отверстия поле имеет дипольный характер. Для расчета момента диполя получены очень простые выражения [3], а поле диполя может быть рассчитано в любой системе координат, в том числе в декартовой.

Следовательно, анализ проникновения помехового поля через круглое отверстие в экране может быть выполнен без существенных затруднений на основе хорошо известных публикаций.

Необходимо отметить, что упомянутый в докладе метод Бете справедлив для помеховых электромагнитных полей, находящихся в сравнительно узкой полосе частот. Если электромагнитное поле имеет очень широкую полосу частот от единиц Гц до единиц ГГц, то необходимо использовать расчетные методы, основанные на известном в теории дифракции интеграле Кирхгофа [6]. Такой полосой частот обладают электростатический разряд и электромагнитные импульсы преднамеренного воздействия. Применение интеграла Кирхгофа для расчета проникновения таких импульсов через отверстия в экранах впервые обосновано в [7].

Литература

1. Аполлонский, С.М. Расчет сложных электромагнитных экранирующих конструкций / С.М. Аполлонский.– М.: РУСАЙНС, 2011. – 554 с.
2. Князев, А. Д. Конструирование радиоэлектронной и электронно-вычислительной аппаратуры с учетом электромагнитной совместимости / А.Д. Князев, Л.Н. Кечиев, В.В. Петров. – М.: Радио и связь, 1989. – 222 с.
3. Ландау, Л.Д. Теоретическая физика: в 12 т. / Лифшиц. – 7-е изд., испр. – М.: Наука, 1982. – Т. 8. Электродинамика сплошных сред. – 620 с.
4. Джексон, Дж. Классическая электродинамика / Дж. Джексон. – М.: Мир, 1965. – 702 с.
5. Уфлянд, Я.С. Метод парных уравнений в задачах математической физики / Я.С. Уфлянд. – Л.: Наука, 1977. – 220 с.
6. Шимони, К. Теоретическая электротехника / К. Шимони. – М.: Мир, 1964. – 713 с.
7. Бочков, К. А. Элементы моделирования электромагнитной совместимости устройств железнодорожной автоматики и телемеханики / К. А. Бочков, Д. В. Комнатный. – Гомель: БелГУТ, 2013. – 185 с.

ИССЛЕДОВАНИЕ СРЕДСТВ ЗАЩИТЫ ТЕЛЕФОННОГО АППАРАТА ОТ УТЕЧКИ ПО АКУСТОЭЛЕКТРИЧЕСКИМ КАНАЛАМ НА ВИРТУАЛЬНЫХ ЛАБОРАТОРНЫХ СТЕНДАХ

О.Р. ЛУКМАНОВА

*Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет “Московский институт электронной техники”»,
г. Зеленоград, Россия*

Введение

Акустоэлектрические каналы являются одними из наиболее опасных технических каналов утечки акустической речевой информации из выделенных помещений (ВП), так как позволяют перехватывать речевую информацию без проникновения в пределы контролируемой зоны (КЗ) объектов [1].

Причиной возникновения акустоэлектрических каналов утечки информации являются вспомогательные технические средства и системы (ВТСС), устанавливаемые в ВП, среди которых наиболее часто встречаются телефонные аппараты [2].

Для защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам используются пассивные и активные способы защиты. К пассивным способам защиты ВТСС относятся: ограничение сигналов малой амплитуды и фильтрация высокочастотных сигналов (реализуется в устройстве защиты «Гранит-8»), отключение акустоэлектрических преобразователей (реализуется в устройстве защиты «МП-8»). Активные способы защиты от утечки информации по акустоэлектрическому каналу предусматривают подачу в линию маскирующего шумового сигнала речевого диапазона частот (реализуется в устройстве защиты «МП-1А») [2].

Устройство защиты должно обеспечивать защиту телефонного аппарата от утечки речевой информации, возникающей как вследствие акустоэлектрических преобразований, так и «высокочастотного навязывания» [2].

Вопросы, связанные с изучением способов и средств защиты речевой информации от утечки по акустоэлектрическим каналам, рассматриваются в дисциплине «Защита информации от утечки по техническим каналам», которая включена в базовую часть федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) по направлению подготовки 10.00.00 Информационная безопасность. Стоимость лабораторного стенда для изучения данных вопросов составляет более 3 000 000 рублей. Одним из возможных направлений снижения стоимости лабораторного оборудования в процессе обучения студентов является использование при проведении лабораторных работ методов имитационного моделирования. Для этих целей авторами была выбрана среда проектирования электронных схем NI Multisim.

Целью работы является с использованием виртуального лабораторного стенда провести исследование основных характеристик типовых устройств защиты от утечки информации по акустоэлектрическому каналу и проведена оценка их работоспособности при подключении к телефонной сети.

1. Исследование характеристик пассивных средств защиты информации

Для исследования амплитудно-частотной характеристики устройства защиты в режиме защиты от утечки информации, возникающей за счет акустоэлектрического преобразования акустических сигналов в электрические на вход устройства подадим сигнал, напряжением $U = 0,1$ В, и на выходе устройства измерим затухание сигнала в диапазоне частот от 1 Гц до 10 кГц с использованием встроенной функции AC Sweep в NI Multisim.

Для исследования амплитудно-частотной характеристики устройства защиты в режиме защиты от «высокочастотного навязывания» с помощью имитатора аппаратуры «высокочастотного навязывания» со стороны АТС в линию подадим сигнал амплитудой $U = 5$ В, и на выходе устройства (точка К1) измерим затухание сигнала в диапазоне частот от 10 кГц до 10 МГц с использованием встроенной функции AC Sweep в NI Multisim.

На основе изучения описания средства защиты «Гранит-8» [2] была спроектирована модель этого устройства, представленная на рисунке 1. Входными модулями устройства защиты являются два диодных ограничителя сигналов малой амплитуды (1), которые обеспечивают подавление низкочастотных сигналов, возникающих в телефонном аппарате вследствие акустоэлектрических преобразований речевых сигналов. Выходным модулем устройства защиты (2), является два П-образных LC-фильтров нижних частот, которые обеспечивает подавление высокочастотных сигналов «навязывания».

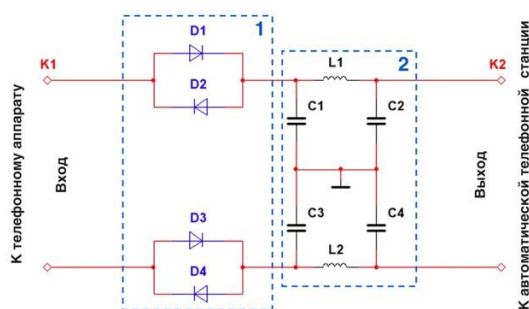


Рисунок 1. – Имитационная модель средства защиты телефонных аппаратов «Гранит-8»

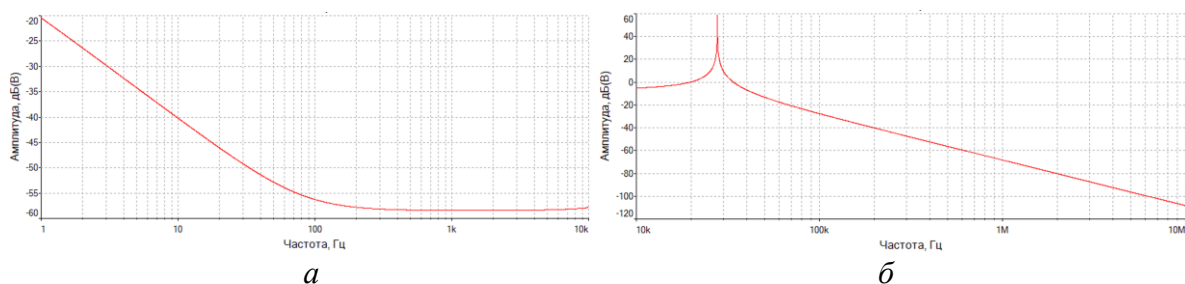


Рисунок 2. – Амплитудно-частотная характеристика модели устройства защиты «Гранит-8» в режимах: *a* – ограничения сигналов малой амплитуды; *б* – подавления сигналов «высокочастотного навязывания»

Анализ амплитудно-частотной характеристики макета устройства защиты «Гранит-8» в режиме ограничения сигналов малой амплитуды на рисунке 2 *a* показывает, что в речевом диапазоне частот от 10 Гц до 10 кГц, затухание сигнала амплитудой 0,1 В составляет порядка 58 дБ.

Анализ амплитудно-частотной характеристики макета устройства защиты «Гранит-8» в режиме подавления сигналов «высокочастотного навязывания» (рис. 2 *б*) показывает, что частота среза фильтра составляет – 36,5 кГц, а частота резонанса – 27,7 кГц. На частоте 100 кГц затухание составляет более 30 дБ, а на частотах свыше 600 кГц – более 60 дБ, что обеспечивает подавление высокочастотных сигналов до уровня ниже, чем напряжение открытия диодов D1 – D4, и исключает возможность перехвата информации методом «высокочастотного навязывания».

На основе изучения описания устройства защиты «МП-8» [2] была спроектирована модель, которая включает: блок контроля состояния телефонной сети, электронные ключи и схема вызова устройства. Для работы модели устройства защиты была составлена схема на основе ключей, управляемых напряжением (рис. 3). Звуковую микросхему в вызывной цепи устройства защиты (2) заменили на эквивалентный элемент Buzzer с соответствующим током

потребления. Сигнал «вызов» (звонок) поступает из телефонной линии в специальную автономную схему вызова устройства защиты, который сопровождается звуковым и оптическим сигналом (светодиод зеленого цвета).

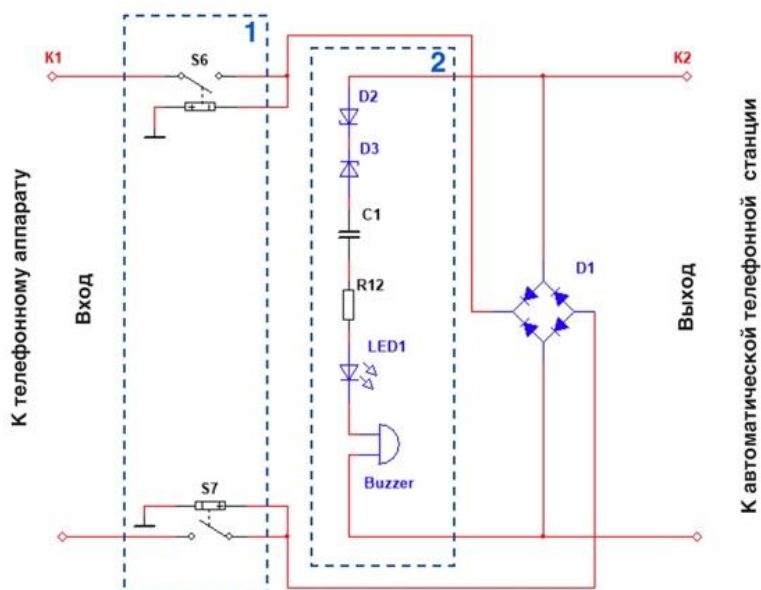


Рисунок 3. – Имитационная модель средства защиты телефонных аппаратов «МП-8»

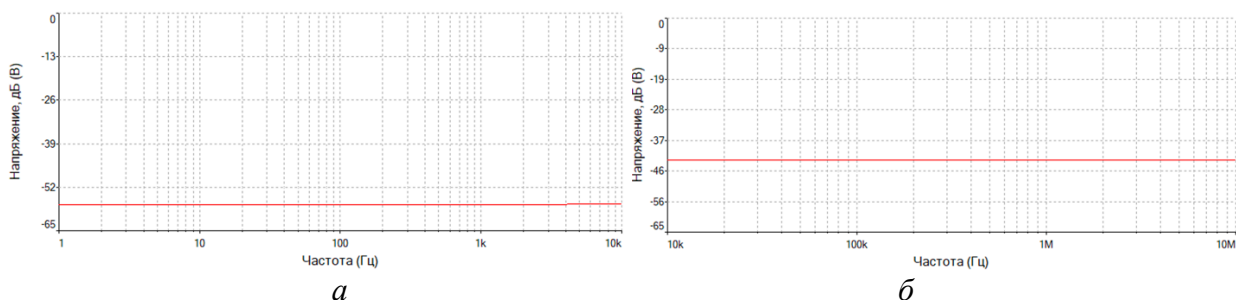


Рисунок 4. – Амплитудно-частотная характеристика модели устройства защиты типа «МП-8» в режимах: а – ограничения сигналов малой амплитуды; б – подавления сигналов «высокочастотного навязывания»

Анализ амплитудно-частотной характеристики макета устройства защиты «МП-8» в режиме ограничения сигналов малой амплитуды (рис. 4 а) показывает, что в речевом диапазоне частот от 10 Гц до 10 кГц, затухание сигнала амплитудой 0,1 В составляет порядка 60 дБ.

Анализ амплитудно-частотной характеристики макета устройства защиты «МП-8» в режиме подавления сигналов «высокочастотного навязывания» показывает, что затухание сигнала в диапазоне частот от 10 кГц до 10 МГц составляет 43 дБ (рис. 4 б).

2. Исследование характеристик активных средств защиты информации

На основе изучения описания устройства защиты «МП-1А» [2] была спроектирована модель активного средства защиты (рис. 5), включающего пассивный модуль защиты (1 и 2), активный модуль защиты (3 и 4) и блок питания и управления (5). Генератор шума состоит источника шума (3) и усилителя (4). Источником шума является стабилитрон $D7$ подключенный в обратном смещении к транзистору $Q2$, благодаря этому включению и возникает белый шум. К источнику шума подключен блок питания $V3$ с напряжением 12 В. Для включения и выключения сигнала с генератора шума при положенной и снятой телефонной трубки соответственно используется блок управления, в данной схеме обозначен $S5$. Исследование пассивного модуля проводится аналогично средства защиты «Гранит-8».

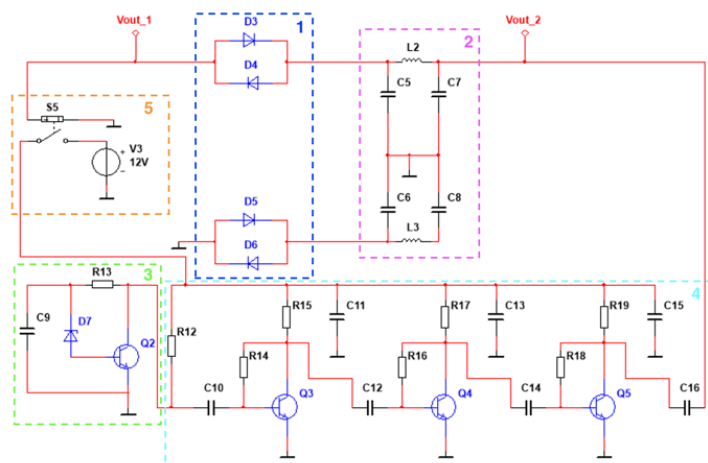


Рисунок 5. – Имитационная модель активного средства защиты телефонных аппаратов

Для исследования эффективности активного модуля защиты используется виртуальный лабораторный стенд (рисунок 5), включающий осциллограф и анализатор спектра, подключаемые к выходу Vout 2. На рисунке 6 представлена осциллограмма шумового сигнала, формируемого генератором шума и его спектрограмма.

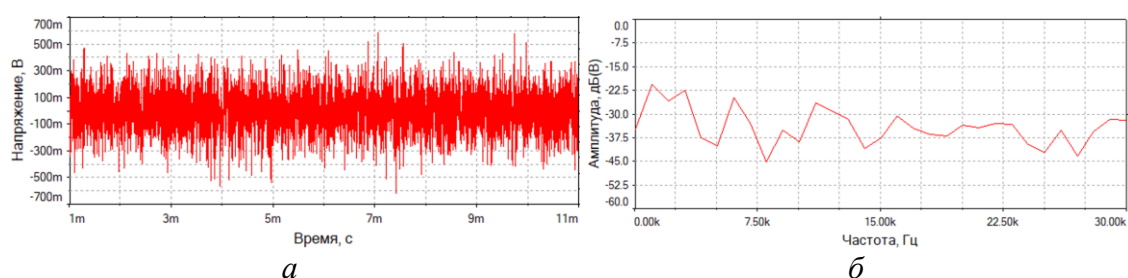


Рисунок 6. – Результаты моделирования шумового сигнала:
а – осциллограмма; б – спектрограмма

Анализ осциллограммы и спектрограммы (рис. б) шумового сигнала показывает, что генератор шума формирует шумовой сигнал в речевом диапазоне частот амплитудой от 12 мВ до 0,5 В.

Одним из показателей маскирующего шума Кш, создаваемого генератором шума, используется энтропийный коэффициент качества шума (ЭККШ), который характеризует приближение закона распределения мощности шума к идеальному «белому» шуму с нормальным законом распределения мощности.

Для исследования качества шума с полученной осциллограммы сигнала была сформирована выборка, состоящая из 100000 значений, измеренная с шагом 140 нс. Для спроектированного устройства значение рассчитанного коэффициента качества шума составило 0,96.

3. Исследование характеристик средств защиты информации с подключением модели телефонной сети

Для исследования основных характеристик средства защиты была спроектирована модель телефонной сети со встроенным модулем телефонного аппарата (1), имеющем в своем составе акустоэлектрические преобразователи (звонковый капсюль (2), динамик (4) и микрофон телефонной трубки (3), подключенной АТС (5) обрабатывающей типовые режимы работы (сигнал вызова, постоянное питание в телефонной линии), а также модель аппаратуры «высокочастотного навязывания» (6), подключенная к телефонной линии (рис. 7). В качестве примера проведем исследование на основе средства защиты «Гранит-8».

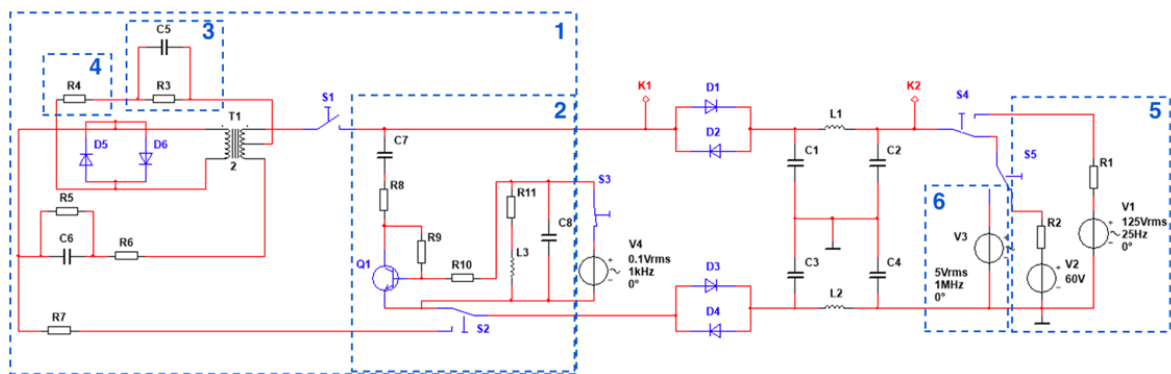


Рисунок 7. – Имитационная модель устройства защиты, подключенная к телефонной сети

Для моделирования акустоэлектрических преобразований малой амплитуды в звонковой цепи телефонного аппарата с помощью имитатора информативного сигнала ($V4$) на вход устройства защиты подадим сигнал на частоте $f = 1$ кГц, напряжением $U = 0,1$ В.

Для моделирования режима «высокочастотного навязывания», с помощью аппаратуры ($V3$, ключ $S5$ замкнут) со стороны АТС в линию подадим сигнал амплитудой $U = 5$ В и частотой 1 МГц.

Измерения проводятся с помощью двухканального осциллографа XSC1 подключенного на входе и выходе устройства защиты в точках $K1$ и $K2$. Анализ полученных осциллограмм показывает, что средство защиты обеспечивает защиту информации от акустоэлектрических преобразований в том числе от «высокочастотного навязывания» (рис. 8).

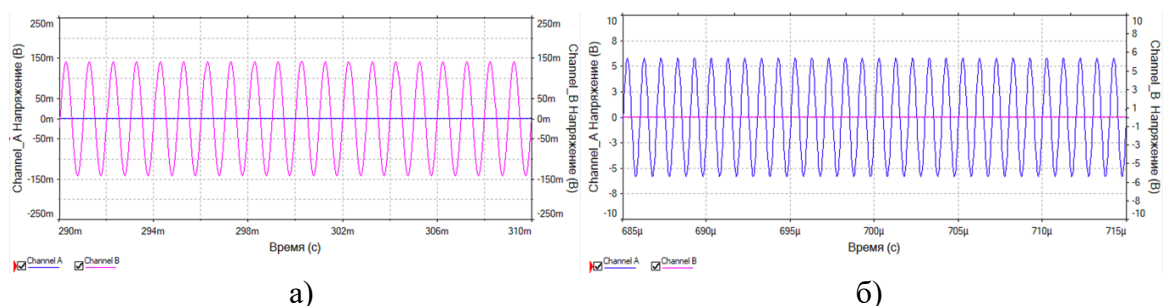


Рисунок 8. – Осциллограммы сигналов на входе и выходе макета устройства защиты (в режимах) ограничения сигналов малой амплитуды; б) подавления сигналов «высокочастотного навязывания»

Заключение

В среде проектирования электронных схем NI Multisim разработаны имитационные модели устройств защиты телефонных аппаратов типа «Гранит-8», «МП-8» и «МП-1А», модель телефонной сети и виртуальные лабораторные стенды для исследования характеристик устройств защиты. С использованием виртуальных лабораторных стендов проведено исследование основных характеристик разработанных устройств защиты и оценена их работоспособность при подключении к телефонной сети.

Результаты исследований могут быть использованы при разработке лабораторного практикума по разделам дисциплин, затрагивающим вопросы защиты информации от утечки по акустоэлектрическим каналам.

Литература

1. Хорев А.А. Техническая защита информации: учеб. пособие: В 3 т. Т. 1: Технические каналы утечки информации /А.А. Хорев. – М.: НПЦ «Аналитика», 2008. – 436 с.
2. Хорев А.А. Способы и средства защиты речевой информации от утечки по акустоэлектрическим каналам // Специальная техника. М.: Электрозавод, 2014. – № 1. – С. 48–63

ОБОСНОВАНИЕ ИЗМЕРИТЕЛЬНОГО СИГНАЛА ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ ПРИ ДИСКРЕТНО-КВАНТОВАННОМ ПРЕОБРАЗОВАНИИ

М.М. БАРАНОВСКИЙ¹, А.Г. ФИЛИППОВИЧ¹,
В.К. ЖЕЛЕЗНЯК², С.В. ЛАВРОВ²

¹*Оперативно-аналитический центр при Президенте Республики Беларусь,
г. Минск, 220030, Республика Беларусь*

²*Учреждение образования «Полоцкий государственный университет
имени Евфросинии Полоцкой»,
г. Новополоцк, 211440, Республика Беларусь*

Введение

Использование современных цифровых технологий неразрывно связано с применением аналого-цифровых и цифро-аналоговых преобразователей. 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 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 отдельной оценке аналогового речевого сигнала и речевого сигнала, представленного в цифровой форме при его передаче по линиям связи.

Для оценки защищенности речевой информации могут использоваться следующие измерительные сигналы [2, 3]:

- гармонический, соответствующий требованиям СТБ 34.101.29-2011;
- шумовой во всей полосе речевого сигнала;
- линейно-частотно-модулированный;
- меандровая последовательность;
- частотно-модулированный без разрыва фазы.

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.

Поэтому задачей настоящей работы является обоснование измерительного сигнала для оценки защищенности речевой информации при дискретно-квантованном преобразовании.

Требования к измерительным сигналам для оценки защищенности речевых сигналов при дискретно-квантованном преобразовании

Дискретно-квантованное представление речевых сигналов осуществляют заменой непрерывной шкалы мгновенных значений непрерывного сигнала дискретной шкалой линейно-ломаной аппроксимации. Квантующее устройство является основным преобразующим устройством, содержащим линейный и нелинейный элементы [4]. Идеальным квантующим устройством является нелинейное устройство с нулевой памятью, передаточная характеристика которого представлена ступенчатой функцией с интервалами квантования входного сигнала Δ , находящимися в однозначных соотношениях с кодирующим входным цифровым сигналом с систематической ошибкой квантования, присущей квантующему устройству.

Дискретизация по времени заменяет непрерывную функцию решетчатой, которая определяет совокупность выделенных ординат или дискрет. Если задана непрерывная

функция времени $f(t)$, то ее среднее значение при дискретных значениях аргумента $t = t_n$ преобразуется в решетчатую функцию $f(t_n)$. Разность двух соседних значений аргумента $T_n = t_{n+1} - t_n$ ($t_{n+1} > t_n$) определяет интервал дискретизации (период повторения) по времени, где $n = 1, 2, \dots, m$ [5].

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

$$SNR = 6,02N + 10 \lg \left(\frac{F_d}{2\Delta f_B} \right) + C_s, \quad (1)$$

где C_s – постоянная, учитывающая форму входного (измерительного) сигнала (для гармонических сигналов $C_s = 1,7$ дБ, для звуковых сигналов $C_s = -15 \dots +2$ дБ).

Основными формами (типами) сигнала являются:

- синусоидальный (косинусоидальный);
- прямоугольный (меандр);
- пилообразный (нарастающий или спадающий);
- треугольный.

При равномерном квантовании по уровню из-за нелинейности гармонического сигнала по форме шум квантования не является равномерным в течение периода гармонического сигнала, что не позволяет использовать его в качестве измерительного сигнала (рис. 1). Поэтому наиболее оптимальным является использование линейно нарастающего или линейно спадающего сигнала, которыми являются сигналы треугольной и пилообразной формы. Возникающий при этом шум квантования имеет пилообразную форму, что повышает чувствительность его обнаружения.

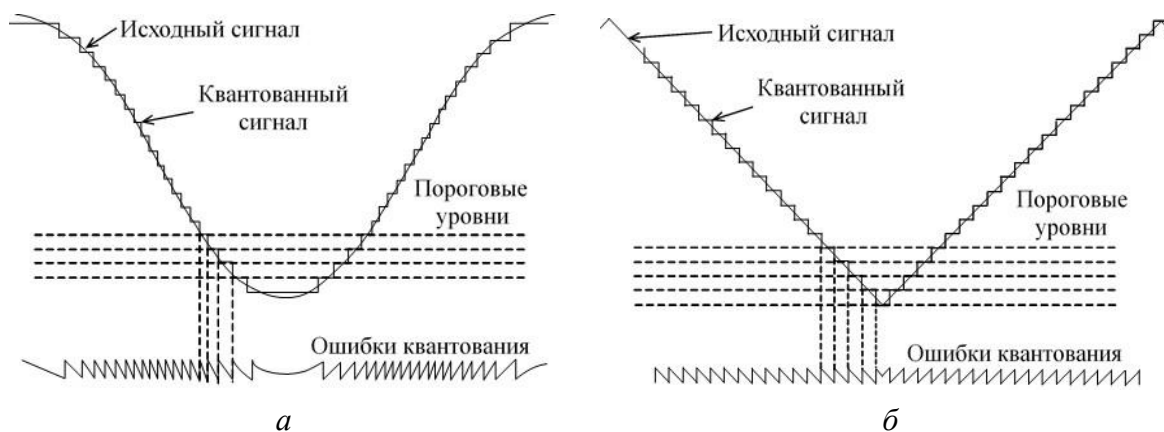


Рисунок 1. – Квантование сигнала: *a* – косинусоидального; *б* – треугольного

Для определения преимуществ некоторых сигналов для их использования в качестве тестовых остановимся на рассмотрении их характеристик. Разложение периодической импульсной последовательности треугольной формы в ряд Фурье имеет следующий вид [5]:

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

где A – амплитуда сигнала; k – номер гармоники ($k = 1, 3, 5, \dots$); $\omega = \frac{2\pi}{T_{\Pi}}$ – угловая частота сигнала; T_{Π} – период сигнала.

Разложение импульсов пилообразной формы в ряд Фурье имеет следующий вид [5]:

$$f(t) = \frac{A}{2} - \frac{A}{\pi} \sum_{k=1}^{\infty} \frac{1}{k} \sin k\omega t, \quad (3)$$

где $k = 1, 2, 3, \dots$

Из формул (2) и (3) 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. Кроме того, использование в треугольном сигнале нарастающего и спадающего фронтов позволяет в два раза увеличить время обработки сигнала по сравнению с пилообразным сигналом.

Синтез измерительного сигнала

Для использования единого нормативного критерия разборчивости речи в аналоговой форме речевого сигнала и его дискретно-квантованным представлением предложено для формирования измерительного сигнала в качестве исходного (нормированного) сигнала использовать 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 $\tau = \frac{T}{2}$, $F_i = 250; 500; 650; 800; 950; 1125; 1300; 1500; 1700; 1875; 2050; 2250; 2425; 2725; 3100; 3500; 3850; 4550; 6150; 8600$ Гц.

Для преобразования периодической импульсной последовательности прямоугольной формы в периодическую импульсную последовательность треугольной формы используется автокорреляционная функция. 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 $\tau = 2000; 1000; 769; 625; 526; 444; 385; 333; 294; 267; 243; 222; 206; 183; 161; 143; 130; 110; 81; 58$ мкс.

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

Таким образом, для повышения достоверности оценки защищенности канала утечки речевых сигналов при дискретно-квантованном преобразовании предложено использование измерительного сигнала треугольной формы. Использование предложенного измерительного 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. При этом оценка защищенности аналогового и дискретно-квантованного речевого сигнала будет производиться по единой методике.

Литература

1. Железняк, В.К. Синтез измерительного композитного сигнала для оценки защищенности речевых сигналов при дискретно-квантованном преобразовании / В.К. Железняк, С.В. Лавров, А.Г. Филиппович, М.М. Барановский // Доклады БГУИР. – 2020. – № 18(6), – С. 81–87.
2. Железняк, В.К. Защита информации от утечки по техническим каналам: учеб. пособие / В.К. Железняк. – Санкт-Петербург: ГУАП, 2006. – 188 с.
3. Железняк, В.К., Системный подход: защита информации, помехозащищенность, помехоустойчивость / В.К. Железняк, Д.С.Рябенко, С.В. Лавров // Вестник Полоцкого государственного университета, 2016. – № 4. – С. 2–7.
4. Шкритек, П. Справочное руководство по звуковой схемотехнике / П. Шкритек. – Москва: Мир, 1991 – 446 с.
5. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – Москва: Вильямс, 2007. – 1104 с.

ВОЛОКОННО-ОПТИЧЕСКИЕ ЗАКЛАДКИ В МОДЕЛИ УГРОЗ РЕЧЕВОЙ ИНФОРМАЦИИ

В.В. ГРИШАЧЕВ¹, А.Д. ЗАБОЛОТСКАЯ²

*¹ Российский государственный гуманитарный университет,
Институт информационных наук и технологий безопасности,
г. Москва, Россия*

² Softline Company, г. Москва, Россия

Введение

Волоконная оптика является основной технологической базой существующих и будущих информационных систем передачи. Связанные с ней технические каналы утечки информации высоко информативны и опасны. Одним из таких каналов является волоконно-оптический канал утечки речевой информации, суть которого сводится к формированию информативного оптического сигнала в оптоволокне при воздействии информационного речевого сигнала. В структуре канала утечки выделяются средства технической разведки (например, оптический рефлектометр с элементами подключения к оптоволокну), штатной кабельной системы объекта разведки и участков кабеля с повышенным акустическим контактом с окружающей средой объекта. Каждый элемент канала утечки имеет важное значение, например, выбирая средства технической разведки, можно повысить его эффективность, на которое влияет и расположение штатной оптической кабельной системы. Особую роль играет участки оптического кабеля с повышенном акустическим контактом с окружающей средой, к которым относятся любые оптические неоднородности с изменением показателя преломления и/или коэффициента поглощения. Участок с измененными оптическими параметрами (оптическими неоднородностями) обладает повышенной чувствительностью ко всем воздействиям внешних физических полей, вызывающих модуляцию проходящих и отражаемых световых потоков по всем параметрам оптического излучения – амплитуде, частоте, фазе, поляризации и приводящее к созданию канала утечки на основе сформированного информативного сигнала.

По определению [1] закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации). В соответствии с определением, оптические неоднородности вполне можно отнести к пассивным волоконно-оптическим закладочным устройствам (закладкам) и их анализ образования, влияния на функционирование волоконно-оптических каналов утечки информации, в том числе речевой информации, представляется важным.

Пассивным волоконно-оптическим закладочным устройством можно назвать любые структурные изменения оптических свойств пассивных элементов/частей волоконно-оптической кабельной системы, приводящей к повышению чувствительности параметров оптического излучения в оптоволокне к внешним физическим полям и воздействиям, таким как акустическое, электромагнитное и другие поля.

1. Классификация волоконно-оптических закладок

Установка закладок связана с изменением оптических свойств оптоволокна, которые могут быть произведены различным способом и на различных этапах создания волоконно-оптической системы, сами неоднородности могут иметь различную природу образования и оптических свойств. От всех особенностей зависит опасности работы канала утечки и эффективность систем защиты информации. Классификацию пассивных волоконно-оптических закладочных устройств по многим параметрам, один из основных которых

физические характеристики, которые определяют эффективность отклика на воздействие внешних физических полей.

Физические характеристики пассивных волоконно-оптических закладок:

- величина оптической неоднородности – разница показателя преломления или коэффициента поглощения в основной части волокна и внутри неоднородности, градиент оптической неоднородности на границе;

- размеры – поперечное сечение определяется сечением оптоволокна (порядка 125 мкм вместе с оболочкой), длина по оптоволокну (влияет на выбор длины когерентности зондирующего излучения, чем длиннее неоднородность, тем выше когерентность зондирующего излучения для выполнения условия фазового синхронизма), геометрическая форма оптоволокна (изгиб с превышением предельных значений, скрученность и т.д.);

- внутренняя структура – неизменное значение или периодическое изменение оптических параметров внутри неоднородности, например, решетка Брэгга внутри волокна;

- чувствительность к физическим полям – легирование оптоволокна различными химическими элементами приводит к локальному изменению не только показателя преломления или коэффициента поглощения, но и электрооптических, акустооптических и других свойств, повышающих чувствительность к физическим полям.

Физические параметры оптической неоднородности (закладки) влияют на величину формируемого обратно распространяющегося оптического излучения и его глубину модуляции по амплитуде, фазе, частоте, поляризации, что определяет возможности оптической рефлектометрии как средства технической разведки.

Деление закладок можно проводить по различным параметрам, в том числе по физическим характеристикам, а также по этапам появления. Конструктивные изменения пассивных элементов оптической сети могут быть произведены при изготовлении, при установке, при эксплуатации оптической сети, каждая из которых имеет свои особенности и возможности, что позволяет произвести разделение угроз по трем направлениям:

- *волоконно-оптические закладки производства* – при производстве оптических элементов изготовитель может внести изменения в конструкцию пассивных элементов, которые не влияют на его функциональные возможности, но повышают чувствительность к внешним физическим полям. Например, создание брэгговских решеток в сердцевине волокна с длиной волны резонансного отражения на длинах волн в области поглощения материала волокна непосредственно на производстве;

- *волоконно-оптические закладки установки* – в процессе внутри объектного монтажа волоконно-оптической структурированной кабельной системы путем преднамеренного или непреднамеренного нарушения требований по выполнению работ могут быть изменены восприимчивость кабельной системы к внешним воздействиям, которые могут быть, в том числе изначально не известны;

- *волоконно-оптические закладки эксплуатации* – вносятся внутренним нарушителем путем локального механического, теплового, магнитного, электрического другого физического воздействия на кабельные каналы, оптический кабель структурированных кабельных систем защищаемого объекта на стадии эксплуатации оптической сети.

Еще одно деление закладок может быть связано с конструкцией и внутренней структурой волоконно-оптической системой, которая может быть сформирована на различных этапах появления:

- ✓ *внутренние оптические неоднородности* оптического волокна, связанные с существующими неоднородностями, образованными при производстве волокна и кабеля, его монтаже кабельной инфраструктуры и последующей эксплуатации к ним относятся внутренние неоднородности в виде локальных рассеивающих центров, внутренних трещин, внутренних напряжений, неидеальность формы волокна и т.д.; отличительной особенностью данного типа неоднородности является их зависимость от качества используемого кабеля, качества монтажа и эксплуатации;

✓ *инфраструктурные оптические неоднородности и дефекты* связаны с выбором топологии и конструкцией кабельной системы; к ним относятся коммутационные узлы, разъемные и сварные соединения, угловые изгибы и скрутки кабеля, монтажные крепления кабеля и кабельных коробов и т.д.; каждый из элементов характеризуется собственным обратным излучением и потерями на прохождение света, которые существенно зависят от используемых технологий изготовления и установки, размещения, монтажа кабеля;

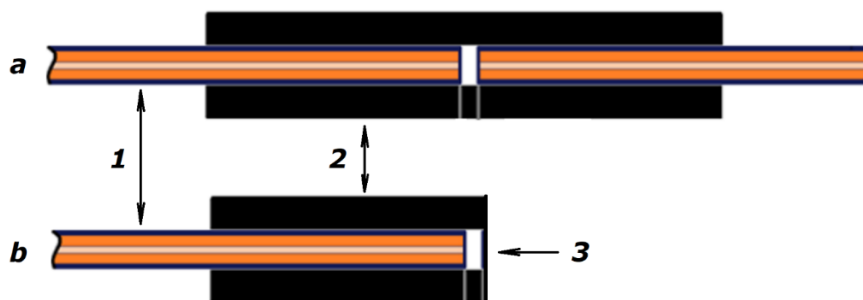
✓ *индуцированные оптические неоднородности и дефекты* вызваны непостоянными внешними воздействиями и полями, которые имеют естественное или искусственное происхождение; их можно разделить на два вида: механические воздействия на оптический кабель и воздействие внешних физических полей: (1) различные изгибы, растяжения-сжатия, скручивание, которым может быть подвержен кабель с целью повышения чувствительности к внешним информативным полям, (2) акустические поля, электромагнитные поля, тепловое воздействие, радиация и др.

Последняя классификация закладок позволяет заявить о существовании «штатных» и «нештатных» закладок, т.е. тех, которые существуют вследствие конструктивных особенностей волоконно-оптической системы (например, сварные участки, изгибы и т.д.) и тех, которые сформированы нарушителем (например, изгибы с превышением предельных значений, воздействие электрическим полем и т.д.). Особую опасность несут индуцированные нарушителем оптические неоднородности, например, путем перетяжки кабеля, размещением источников ядерного излучения вблизи кабеля и другие воздействия, формируемые на различных этапах формирования волоконно-оптической системы.

2. Моделирование пассивных волоконно-оптических акустических закладок

Одна из наиболее опасных угроз безопасности информации на объектах с волоконно-оптическими технологиями является волоконно-оптический канал утечка речевой информации [2], в которой важную роль играют закладочные устройства. Они могут быть штатной частью оптической сети объекта, такие как само оптоволокно в кабельном канале, разъемные соединения и другие элементы штатной сети. А также, они могут быть сформированы нарушителем, такие изгиб/перетяжка кабеля с образованием деформации оптоволокна, манипуляции с элементами оптической сети.

Например, простая модификация волоконно-оптического коннектора. Разъемное соединение кабеля (рис.1 а) с помощью коннекторов является эффективной механической колебательной системой с высокой чувствительностью к воздушным и структурным информативным акустическим волнам с микрофонным эффектом [3]. Но и не включенный в замкнутую оптическую линию кабель с коннектором может стать волоконно-оптическим закладочным устройством с микрофонным эффектом. Стандартный волоконно-оптический микрофон с амплитудной модуляцией промышленного изготовления имеет преобразователь с оптической схемой в виде торца оптоволокна, закрытого легкой отражающей мембраной (рис. 1 б). При воздействии звуковой волны мембрана колеблется и смещается относительно торца, что приводит к модуляции светового потока.



Закладочное устройство, повторяющее конструкцию волоконно-оптического микрофона, можно изготовить на основе коннектора (рис. 2), в конструкции которого для защиты от пыли используется защитный колпачок. В стандартной ситуации не включенный в оптическую сеть оконцованный кабель внутренней прокладки является устройством подверженный преобразованию в волоконно-оптический микрофон. Закладочным устройством в этом случае является модифицированный колпачок, в котором внутренняя часть дна покрывается отражающим покрытием или прослойкой из тонкой пленки, выполняющей роль мембраны. Надо отметить, что сам надетый на ферулу колпачок без каких-либо модификация повышает чувствительность торца к звуковым волнам. Закладочное устройство в виде модифицированного колпачка трудно обнаружить, и его установка обязательна при эксплуатации.

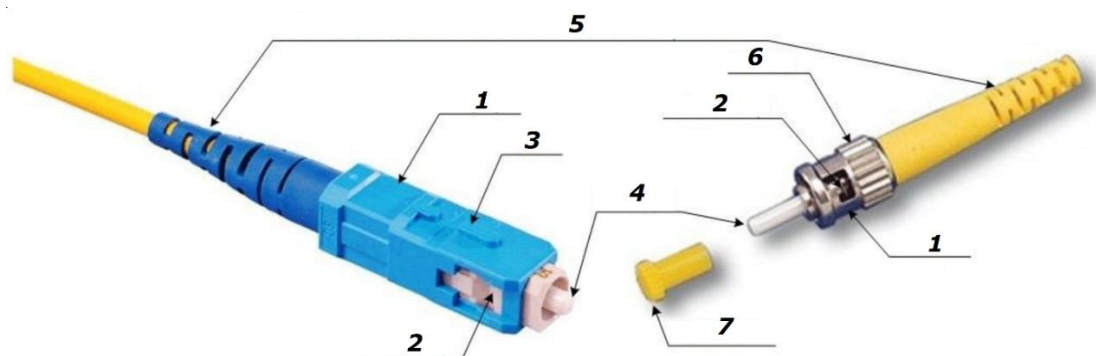


Рисунок 2. – Конструкция коннектора типа SC и ST: 1 – корпус; 2 – фиксатор; 3 – ключ; 4 – ферула; 5 – хвостовик; 6 – зажим; 7 – пылезащитный колпачок

Практическая демонстрация работы некоторых «штатных» и «нештатных» волоконно-оптических закладочных устройств проведена на небольшом количестве видов закладок методом артикуляционных измерений по оптической схеме на отражение с помощью двух волоконно-оптических тестер-телефонов РУБИН 021 с амплитудной оптической модуляцией (рис. 3). Объект исследования (2) размещался в малогабаритной звукоизолирующей камере (коэффициент звукоизоляции менее 20 дБ) с динамиком (1). Оптическое зондирование осуществлялось одним тестер-телефоном РУБИН 021 как источник и другим как приемник (4) через разветвитель (3) с одним входом и двумя выходами с делением 50 %/50 %. Два тестера-телефона использовались для исключения самовлияния при работе только с одним. Принятый звуковой сигнал дополнительно усиливался (5) и выводился на осциллограф (7) для визуального контроля и на наушники для прослушивания оператором.

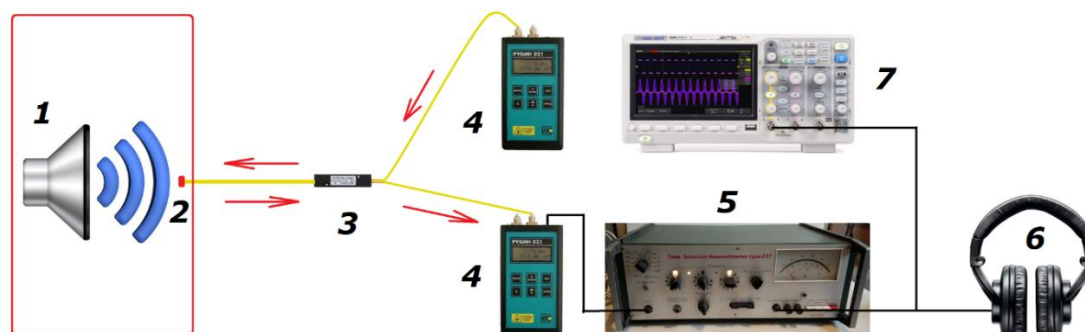


Рисунок 3. – Блок-схема экспериментальной установки по исследованию волоконно-оптических закладок: 1 – источник звука в звукоизолирующей малогабаритной камере; 2 – объект исследования (закладка); 3 – волоконно-оптический разветвитель 1×2; 4 – волоконно-оптические тестер-телефоны Рубин 021; 5 – селективный усилитель (селективный нановольтметр UNIPAN 277); 6 – наушники оператора; 7 – цифровой осциллограф

В качестве волоконно-оптических закладочных устройств использовались простейшие конструкции: деформированный кабель и манипуляции с защитным колпачком. Основой для демонстрации волоконно-оптического закладочного устройства являлось простейшая модификация колпачка – верхняя часть колпачка срезалась и цилиндрическое кольцо от колпачка использовалась как фиксатор тонкой фольги на феруле коннектора. Такая конструкция является простейшей демонстрацией работы волоконно-оптического микрофона. Оценка производилась на слух одним оператором по качеству получаемого сигнала: плохо (речь не прослушивалась), удовлетворительно (речь прослушивается без понимания смысла) и хорошо (речь прослушивается, можно понять смысл некоторых слов). Результаты исследования представлены в таблице 1.

Таблица 1. – Результаты исследования

Тип закладки	Эффективность	Особенности
Деформированный кабель		<ul style="list-style-type: none"> • высокая случайность прослушивания речи; • низкая повторяемость; • сильное влияние структурированного звука, т.е. контакта твердой поверхностью; • влияние длины волны зондирующего излучения; • влияние регистрирующей аппаратуры – полосы усиления, типа наушников и др.
скрутка	Удовл.	
перетяжка	Хорошо	
Коннектор		
без колпачка	Плохо	
с колпачком	Плохо	
с пленкой	Хорошо	

Исследования показали высокое влияние средств технической разведки, структурного звука на эффективность акустооптической модуляции в исследуемом элементе, что связано с физикой формирования модуляции, обсуждаемых более ранних работах.

Заключение

Представлен анализ волоконно-оптических закладочных устройств, показан широкий спектр их формирования, отдельно обсуждаются акустические волоконно-оптические закладочные устройства и некоторые способы формирования. Проведенный анализ показывает высокий уровень угроз данных устройств, который проявляется в эффективности получаемых информативных сигналов, высокой скрытности установки и широкого набора способов формирования.

Литература

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). – ФСТЭК России, 2008.
2. Гришачев В.В., Казарин О.В., Калинина Ю.Д. Физическая модель угрозы утечки акустической (речевой) информации через волоконно-оптические коммуникации. – Вопросы защиты информации, 2018. – № 3. – с. 35–51.
3. Гришачев В.В., Казарин О.В., Калинина Ю.Д. Паразитные акустические модуляции световых потоков в разъемных соединениях оптической сети объекта информатизации. – Вопросы защиты информации, 2018. – № 4. – с. 47–56.

МЕТОД ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ПОКАЗАТЕЛЕЙ ШУМА КВАНТОВАНИЯ АНАЛОГО-ЦИФРОВОГО ПРЕОБРАЗОВАНИЯ

Е.Р. АДАМОВСКИЙ, В.К. ЖЕЛЕЗНЯК, К.Я. РАХАНОВ

*Учреждение образования «Полоцкий государственный университет
имени Евфросинии Полоцкой»,
г. Новополоцк, Республика Беларусь*

Введение

Передача цифровых речевых сигналов (РС) является частью системы комплексной защиты информации [1] и относится к технической защите средств коммуникации [2], которые включают преобразование цифрового РС в аналоговую форму с помощью цифро-аналогового преобразователя (ЦАП) с последующей его передачей. На этапе аналого-цифрового преобразования (АЦП) осуществляются дискретизация и квантование сигнала, излучаются физические поля рассеяния – магнитные и электрические, которые являются информационными параметрами передаваемого сигнала и каналом утечки информации (КУИ). Важной задачей является обеспечение помехозащищенности при передаче широкополосных высококачественных РС в каналах связи. Это обуславливает АЦП, являющееся источником шума квантования (ШК), который рассматривается в качестве нового КУИ в шумах высокого уровня. В [3, 4] оценку защищенности КУИ предлагается выполнять с помощью периодической последовательности импульсов треугольной формы, которая не вносит методических погрешностей, обусловленных нелинейностью ШК. Наиболее эффективные методы оптимального приема детерминированного сигнала – на основе корреляционного приема. Цель исследований – количественная оценка информационных показателей ШК АЦП аналогового РС.

1. Методика оценки информационных показателей

Блок-схема автоматизированной оценки КУИ АЦП приведена на рисунке 1 и включает систему приема-передачи, КУИ, программно-аппаратный комплекс (ПАК). Количественная оценка информационных показателей ШК должна выполняться с помощью автоматизированной системы, так как излучаемые поля имеют малую мощность в шумах высокого уровня, что требует дополнительной обработки и накопления. Система приема-передачи сигнала включает генератор измерительного сигнала (ИС) и ЦАП, который передает ИС в линию связи и на АЦП приемника. В момент преобразования сигнала из аналоговой формы АЦП излучает физические поля, характеризующие КУИ. ПАК включает измерительную антенну и персональную электронно-вычислительную машину (ПЭВМ) со специальным программным обеспечением (ПО).

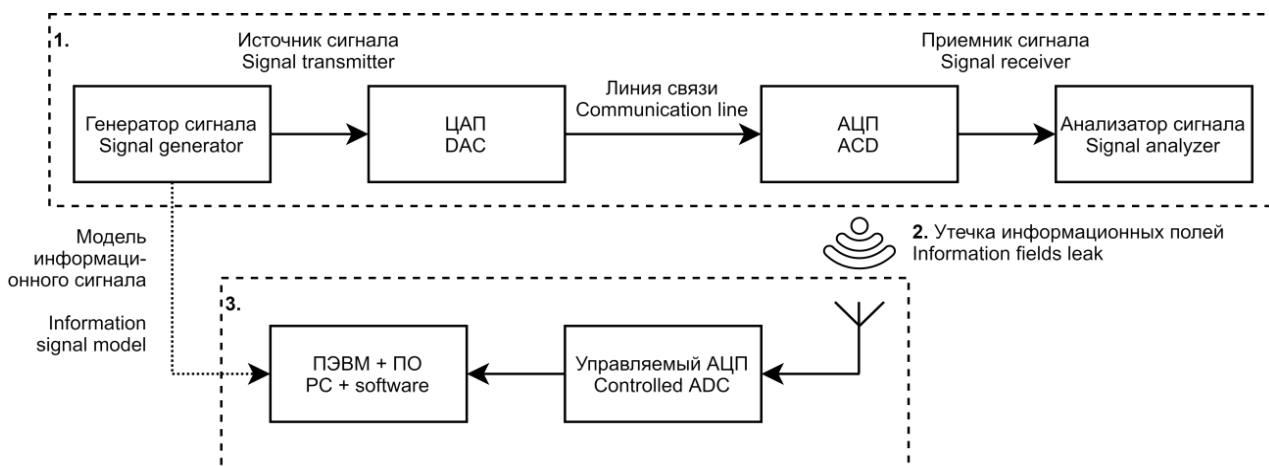


Рисунок 1. – Блок-схема автоматизированной оценки КУИ АЦП

Излучаемые физические поля фиксирует измерительная антенна, а затем передает их через управляемый АЦП для выделения и обработки информационных параметров ИС и ШК с помощью специального ПО на ПЭВМ. В качестве обработки используется синхронное накопление, позволяющее улучшить отношение сигнал/шум (ОСШ).

Алгоритм включает следующие этапы:

1. Формируется модельный (идеальный) ИС в цифровом виде, параметры которого согласованы с генератором сигнала (штриховая линия связи на рисунке 1).
2. Захватывается сигнал с помощью измерительной антенны в точке наблюдения. При передаче сигнала по каналу связи значения фазы и амплитуды сигнала неизвестны, а сам сигнал подвергается искажениям и влиянию шумов.
3. Определяется время задержки ИС путем расчета взаимной корреляции смеси сигнала и шума с модельным сигналом.
4. Рассчитывается ШК путем вычисления разницы принятой смеси сигнала и шума и восстановленной цифровой копией сигнала с учетом фазы.
5. Применяются спектральное накопление и полосовая фильтрация сигналов.
6. Выполняется обнаружение информационных параметров КУИ.
7. Рассчитанные показатели протоколируются и выводятся на экран.
8. Процедура обнаружения информационных параметров повторяется 30 раз, а результаты усредняются; мощность шума увеличивается, измерения повторяются.

Этапы 5 и 6 можно представить в виде спектрального обнаружителя информационных параметров (рис. 2), в котором для более эффективного накопления выполняется преобразование сигнала в частотную область с помощью операции быстрого преобразования Фурье (БПФ) и его разделение на действительную и мнимую части с независимым накоплением и последующим вычислением общего модуля спектральной составляющей. Требуемое количество накоплений до обнаружения сигнала и обнаруженная частота сигнала учитываются в определении исходного уровня информационного параметра.

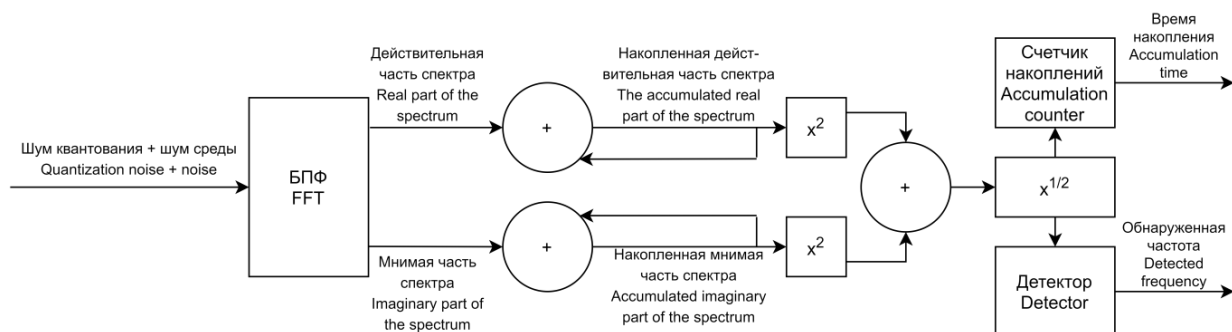


Рисунок 2. – Блок-схема спектрального обнаружителя информационных параметров

В полученном сигнале выполняется поиск максимального элемента, который в спектре шума квантования без аддитивной помехи соответствовал бы его главной гармонике на частоте дискретизации сигнала. Если обнаруженный максимум соответствует частоте дискретизации АЦП, делается вывод о том, что шум квантования накопился и может быть обнаружен над шумами. Постоянная составляющая в виде гармоники на нулевой частоте не учитывается при определении максимума. Записывается количество накоплений, которое потребовалось для выделения гармоники шума квантования при текущем уровне шума среды.

2. Результаты исследований и их обсуждение

Для подтверждения работоспособности предложенного способа обработки и выделения информационных параметров ИС и ШК проведен имитационный натурный эксперимент, в котором вместо измерительной антенны использовался соединительный кабель, подключенный от выхода ЦАП источника сигнала к аналоговому входу управляемого измерительного АЦП (рис. 3).

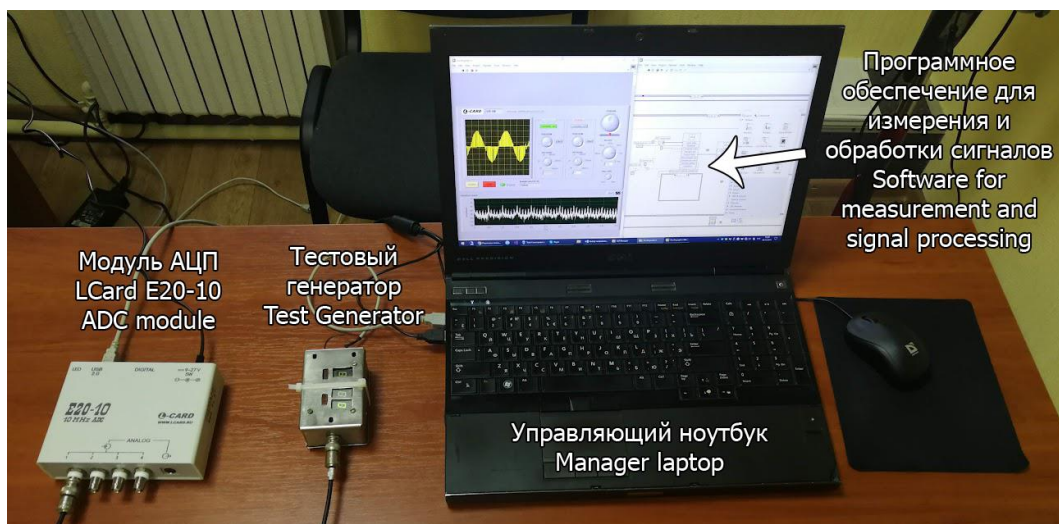


Рисунок 3. – Программно-аппаратный комплекс для обработки и выделения информационных параметров сигнала

Макет включает аппаратную часть и специальное ПО, которое реализует предложенную модель оценки информационных параметров в программной среде LabVIEW. Аппаратная часть включала следующие элементы: ноутбук; управляемый модуль АЦП/ЦАП LCard E20-10; генератор ИС, встроенный ЦАП в ПЭВМ; кабель соединительный АЦП-ЭВМ: аналоговый разъем мини-джек (0,5 м); кабель управления АЦП/ЦАП USB 2.0 тип А-В, длина 1,5 м; источник питания – сетевой адаптер ~ 220 В.

Измерения проводились при изменении количества уровней дискретизации сигнала от 8 ($L = 3$ бита) до 1024 ($L = 10$ бит). Изменение количества уровней дискретизации (разрядности АЦП L) выполнялось программным способом. Предельные значения частоты и уровня сигнала устанавливали с помощью параметрической зависимости между влияющими факторами и контролируемыми параметрами как функция многих переменных при 30 повторениях измерения. В таблице 1 приведены результаты обнаружения частоты и уровня ШК.

Таблица 1. – Результаты обнаружения частоты и уровня шума квантования

Разрядность АЦП, L	Ожидаемая частота, Гц	Обнаруженная частота, Гц	Относительная амплитуда ШК
3	1600	1600	0,6000
4	3200	3200	0,1500
5	6400	6400	0,0400
6	12 800	12 800	0,0180
7	25 600	25 600	0,0050
8	51 200	51 200	0,0010
9	102 400	–	0,0005
10	204 800	–	0,0001

Приведенные в таблице 1 данные показывают, что обнаружение частоты и уровня шума квантования устойчиво выполняется до $L = 8$ бит. При $L = 9$ бит по спектру сигнала возможно судить о наличии ШК, но устойчивого выделения частоты и уровня сигнала не происходит. Для дискретизации при $L = 10$ бит сигнал визуально не наблюдается.

На рисунке 4 представлены графики зависимостей среднего количества накоплений для выделения основной гармоники ШК из фонового шума от количества уровней дискретизации сигнала, сформированного устройством с разрядностью L . За приемлемое (по критерию

времени) количество накоплений возможно оценить лишь некоторые диапазоны ОСШ, при которых гармоники ШК выделяются в пределах 10 итераций.

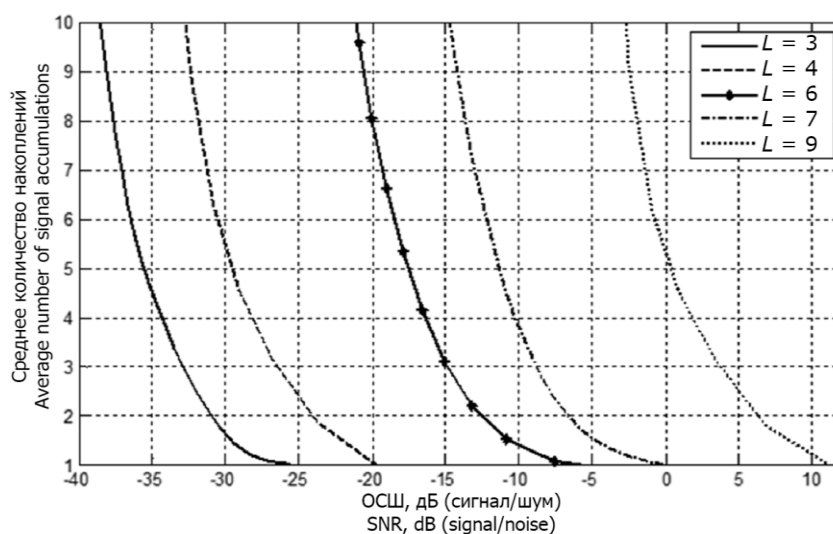


Рисунок 4. – Зависимость количества накоплений для выделения основной гармоники ШК

Анализ рисунка 5 показывает, что при увеличении L, которое снижает уровень гармоник ШК и повышает их частоту, резко возрастает требуемое для выделения количество накоплений сигнала при аналогичном уровне фонового шума. Добавление 1 разряда эквивалентно увеличению числа уровней квантования в два раза и вызывает смещение графика на 7–8 дБ в сторону увеличения ОСШ. Например, при ОСШ минус 20 дБ сигнал с L = 5 может быть накоплен за 8 раз, а сигнал с L = 4 – за один раз.

На рисунке 5 представлены графики зависимостей времени накопления ШК от ширины полосы фильтра. Ограничение полосы фильтра осуществлялось фильтром с заданной полосой вокруг ожидаемого отсчета смеси.

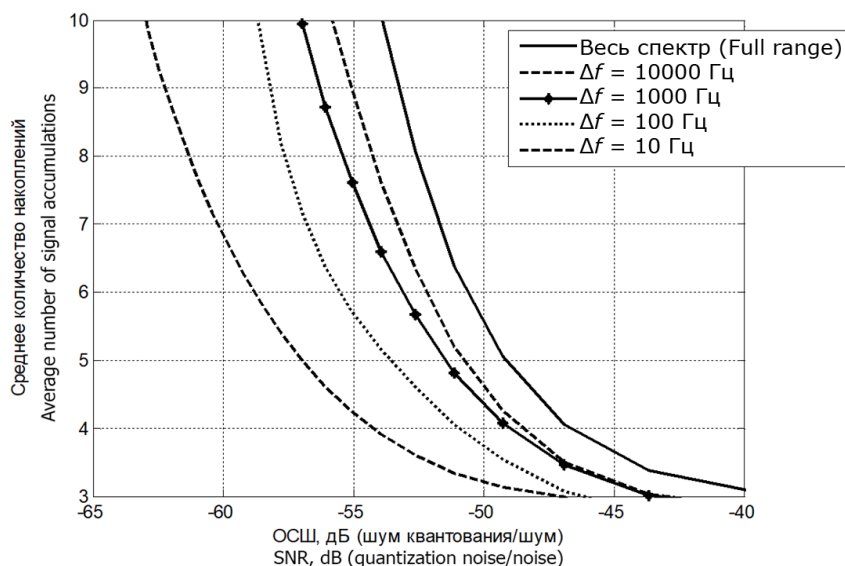


Рисунок 5. – Зависимость времени накопления ШК от ширины полосы фильтра

Из рисунка 5 следует, что сужение полосы в 10 раз позволяет уменьшить время накопления на 10–20 %. Это можно заключить из сравнения графиков, например, при ОСШ минус 55 дБ. Следовательно, сужение полосы накопленной смеси позволяет уменьшить время выделения ШК, что может быть применено на практике перехватчиком сигнала для более быстрого поиска информационных составляющих в шумах при наличии у него сведений

о технических характеристиках целевой системы. Это может позволить ему анализировать лишь ограниченную область частотного спектра.

Заключение

Разработан макет локальной измерительной схемы, с помощью которого проведен имитационный натурный эксперимент оценки информационных показателей ШК АЦП аналогового РС. В качестве информационных показателей КУИ использовались частота дискретизации сигнала и амплитуда ШК.

С помощью макета локальной измерительной схемы выполнен натурный эксперимент, включающий определение параметров информационных составляющих ШК в КУИ путем накопления и анализа сигнала. В результате проведения натурального эксперимента подтверждены гипотезы оценки информационных параметров ШК, получены численные значения информационных параметров.

В результате эксперимента получены зависимости времени накопления от ОСШ ШК/фоновый шум и времени накопления от разрядности АЦП (уровня ШК), которые описывают предельные чувствительности и погрешности детектора информационных параметров, зависимости от контролируемых параметров и влияющих факторов. Уточнение предельных значений оценки информационных параметров необходимо исследовать при подключении измерительных антенн.

Литература

1. Раханов, К.Я. Обеспечение конфиденциальности информации в сети Интернет / К.Я. Раханов, Н.А. Раханов. Новополюцк: Полоц. гос. ун-т, 2021. – 192 с.
2. Железняк, В.К. Защита информации от утечки по техническим каналам / В.К. Железняк. СПб.: Санкт-Петербург. госуд. ун-т аэрокосмич. приборостр., 2006. – 188 с.
3. Анализ ошибки равномерного квантования периодической импульсной последовательностью треугольной формы в спектральной области / В. К. Железняк [и др.] // Проблемы инфокоммуникаций. 2022. – Т. 15, № 1. – С. 39–45.
4. Математическая модель каналов утечки речевых сигналов при дискретно-квантованном представлении / В. К. Железняк [и др.] // Доклады БГУИР. 2020. – Т. 18, № 4. – С. 89–95.

ПЛЕНОЧНЫЕ ОПТИЧЕСКИЕ ЭКРАНЫ ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ВИЗУАЛЬНОЙ ИНФОРМАЦИИ

М.А. БУНЕВИЧ, А.И. МАЙОРОВ,
Т.В. БОРБОТЬКО, И.А. ВРУБЛЕВСКИЙ

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Введение

Утечка информации является серьезной опасностью для организаций и предприятий. Как правило, это происходит в результате умысла третьих лиц или по неосторожности сотрудников организации, что может нанести ущерб государству, обществу и конкретному предприятию. В случае государства такие цели преследует кибертерроризм. Для предприятия целью перехвата информации является получение преимущества в конкурентной борьбе [1, 2]. Создание системы защиты информационных активов от утечки и перехвата должно осуществляться на профессиональном уровне, с использованием самых современных технических средств.

Защитой информации от утечки по визуально-оптическому каналу обеспечивается комплексом мероприятий, полностью исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны при распространении света. Для человека носителем информации об объектах является видимая глазом визуальная информация. С помощью зрения человек получает наибольший объем информации. Визуальный технический способ организации утечки информации позволяет перехватывать или копировать сведения, отражающиеся в визуальной форме, это такие как документы, информация, выведенная на экран монитора компьютера.

Игнорирование систем защиты визуальной информации при работе с компьютером может привести к потере конфиденциальных данных. Поэтому, во многих крупных промышленных и финансовых компаниях используются различные мероприятия технического и организационного характера для сотрудников, чтобы сохранить конфиденциальность корпоративной информации. В первую очередь это влечет за собой использование дополнительных защитных средств, которые делают визуальную информацию недоступной для посторонних.

В случае ЖК-дисплея, ключевым техническим параметром является угол обзора. Способность изменять угол обзора приводит к получению новых возможностей для визуального просмотра отображения информации на экране дисплея. Это позволяет реализовать функции по защите персональной визуальной информации на экране дисплея индивидуального пользователя от нежелательного просмотра сторонних наблюдателей в общественных местах.

1. Метод блокировки света в направлениях, отличных от нормали

Защита от нежелательного просмотра изображения на экране дисплея посторонними лицами затрагивает многих пользователей. Особую актуальность это вызывает при пользовании компьютерными устройствами с дисплеями в публичных местах, таких как в залах ожидания вокзалов или аэропортов, в таможне. Это также распространяется на устройства с большим экраном, например, ноутбуков, платежных и банковских терминалов, а также автоматов, продающих билеты на транспорт.

Способ решения такой задачи лежит в способности ограничить угол обзора так, чтобы информация на экране была видна только владельцу, непосредственно смотрящему на экран под прямым углом. Технически сужение угла обзора можно достичь различными способами. Это за счет изменения электрооптических свойств ЖК-дисплея. В этом случае не требуется разработка новых технологий. Защита информации требуется не все время и поэтому

пользователь должен иметь возможность сохранить режим наблюдения с широким углом обзора. Пользователь должен сам решить вопрос, когда сделать просмотр информации на экране его информационного устройства частным или публичным.

В настоящее время широко используется два базовых метода для регулирования или уменьшения заведомо широкого угла обзора: это сужение контрастной угловой характеристики и блокировка света в направлениях, отличных от нормали.

Для дисплейной структуры применяется дополнительный плоский экран. Дополнительный экран для управления углом обзора расположен поверх панели ЖК-дисплея. В таком экране используется эффект жалюзи на микроуровне. Это позволяет производить блокировку света, проходящего от источника подсветки через ЖК-дисплей в направлениях, отличных от нормального (влево и вправо). Наблюдатели, находящиеся справа и слева, не могут видеть изображение на экране дисплея.

2. Техническая реализация пленочного оптического защитного экрана

Разработанная специалистами БГУИР специальная защитная пленка на экран является эффективным средством для обеспечения конфиденциальности визуальной информации. Для простого пользователя в этом случае все предельно просто. Он наклеивает пленку на экран дисплея, и уже никто не сможет увидеть, чем вы занимаетесь на вашем ноутбуке.

С точки зрения технологии защитная пленка напоминает жалюзи, только в роли пластин-ламелей выступают система канавок, заполненных черной массой на микроуровне в оптической пленке.

На вид экран выглядит как пластичная и тонкая пленка черного цвета, которая крепится к экрану дисплея. Ее можно установить для работы на удалении или на время командировки. При необходимости она легко снимается. Материал подобного экрана является аналогом собственной разработки материала ALCF – Vikuiti™ Advanced Light Control Film Anti-glare 60° (3M). Это оптическая пленка, которая выполняет функцию ограничителя светового потока, проходящего под углами более 60°. Для внешнего слоя пленки использован поликарбонат, а материалом для внутреннего слоя с пленками-перегородками выступает углеродная масса. Вид на такой оптический защитный экран в микроскопе под большим увеличением показан на рисунке 1.

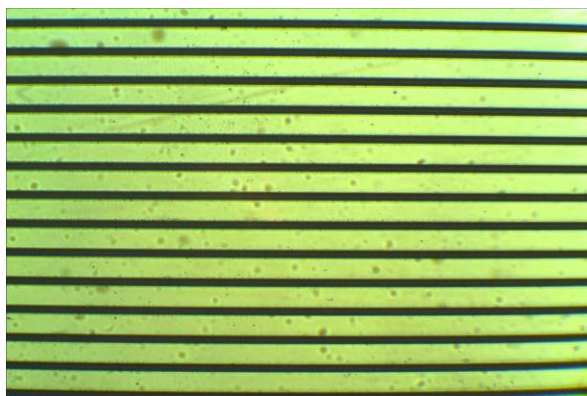


Рисунок 1. – Оптический защитный экран при просмотре под большим увеличением в микроскопе

В основе работы такого оптического фильтра используются мини-жалюзи, встроенные в пленку, которые уменьшают просмотр экрана под углом в 25° и практически полностью зачерняют изображение под углом в 45°. Защищает информацию при просмотре с двух направлений – слева и справа.

Разработан специальный состав светопоглощающего полимерного материала и технология его нанесения и полимеризации в системе глубоких канавок в прозрачном полимерном носителе.

Визуализация принципа работы такого защитного экрана показана на рисунке 2.

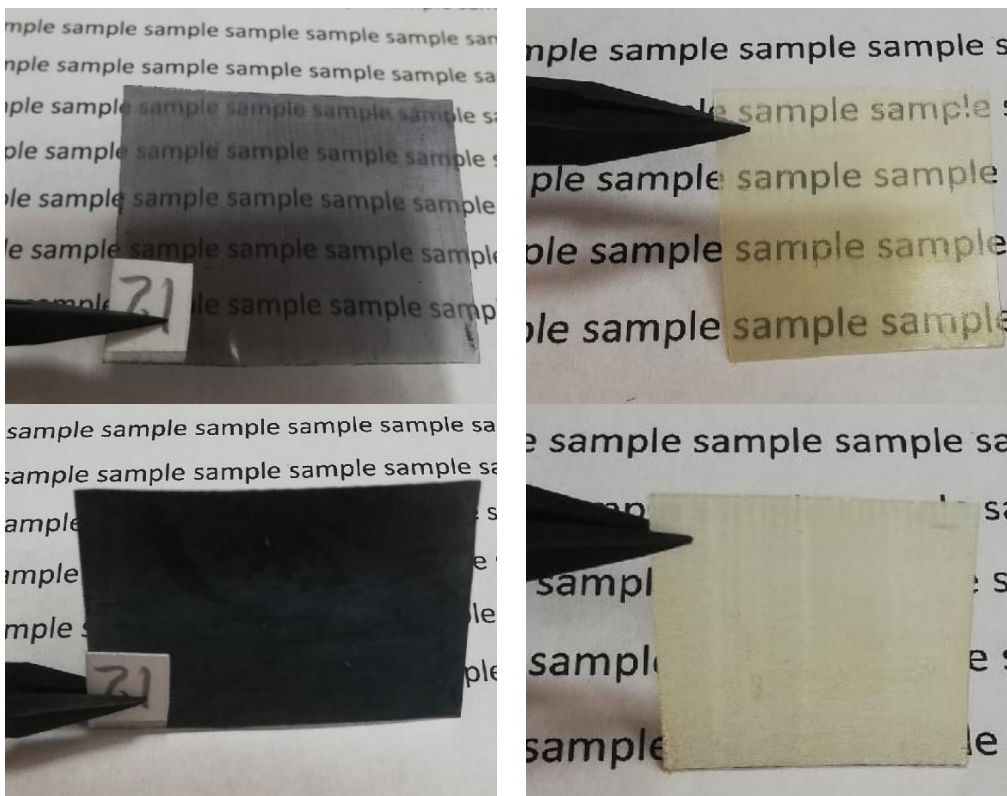


Рисунок 2. – Примеры реализации оптического фильтра

Плоские экраны предназначены для сохранения конфиденциальности информации, отражаемой на мониторах, дисплеях и индикаторных панелях. Обеспечивает защиту информации от несанкционированного съема посторонними людьми, находящимися за пределами угла обзора в 10 и более градусов.

Заключение

1. Разработанный специалистами БГУИР пленочный экран представляет собой двустороннюю оптически прозрачную пленку, изготовленную с использованием инновационной технологии «микрожалюзи». Пленка обладает антибликовым эффектом и уменьшает отражение света, за счет чего позволяет комфортно пользоваться устройством при интенсивном освещении в помещении.

2. Преимущества использования пленочного экрана:

- снижает напряжение на глаза пользователя за счет создания контрастности мелкого текста и изображений;
- не искажает отображение информации на дисплее;
- легко устанавливается и снимается;
- защищает дисплей от внешних повреждений и пыли.

3. Рабочий диапазон длин волн (оптический) – 350–800 нм.

4. Пленочный экран может быть востребован для устройств, используемых работниками банковской сферы, пограничного контроля, таможенной службы и др.

Литература

1. О защите персональных данных: Закон Республики Беларусь от 7 мая 2021 г. № 99-З: принят Палатой представителей 2 апреля 2021 г.: одобрен Советом Республики 21 апреля 2021 г. // Нац. Прав. Инт.-пор. Республики Беларусь, 14.05.2021, 2/2819.

2. О противодействии терроризму: федер. закон Рос. Федерации от 27 июля 2006 г. № 152-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 8 июля 2006 г.: одобрен Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г. // Рос. газ., 29.07.2006, № 4131.

ЗАСЕДАНИЕ № 2 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СОЮЗНОГО ГОСУДАРСТВА БЕЛАРУСИ И РОССИИ

УДК 004.056

ОЦЕНКА ДОСТУПНОСТИ СИСТЕМЫ ЭДО, РЕАЛИЗОВАННОЙ НА БАЗЕ СОБСТВЕННОЙ ИТ-ИНФРАСТРУКТУРЫ

И.И. ЛИВШИЦ

Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО» (Университет ИТМО), г. Санкт-Петербург, 197101, Российская Федерация

Часть 1. Объект исследования

Объектом исследования являются системы электронного документооборота (ЭДО), предназначенные для работы внутри корпоративной информационной системы (КИС) для обработки информации, отнесенной в установленном порядке к персональным данным (ПДн) или коммерческой тайне (КТ) в соответствии с применимым законодательством в Российской Федерации. Объем применимого законодательства ограничен ФЗ-98, ФЗ-152, Постановлением Правительства № 1119, приказами ФСТЭК России в части требований к системам защиты информации (СЗИ) и ФСБ в части требований к системам криптографической защиты информации (СКЗИ).

Часть 2. Текущее состояние объекта исследования

Известно, что, несмотря на доступность некоторых типовых решений, имеются существенные неразрешимые системные противоречия, например, между обеспечением безопасности, удобства, интероперабельности, достоверности и пр. Как было показано в некоторых публикациях, до сих пор не было представлено эффективное решение, обеспечивающее риск-ориентированный подход для проектов ЭДО с доказанной безопасностью. Длительное время в Российской Федерации применялись решения ЭДО, построенные на иностранных ИТ-компонентах (SAP, Oracle), при этом вопросы информационной безопасности (ИБ) решаются в основном с использованием систем управления базами данных (PostgreSQL, Microsoft SQL Server, Oracle и др.), операционных систем (Windows, различные клоны Linux) и т.д. Выявленные противоречия (между стоимостью ЭДО и наложенных СЗИ / СКЗИ; уровнем ИБ, удобством конечного пользователя и пр.) объективно потребовали применения нового решения. В ряде публикаций отмечалось, что для перехода на ЭДО не хватает стандартов и регламентов¹.

В определенной мере существенным драйвером развития ЭДО в современных условиях могут быть облачные технологии, в частности, по оценкам экспертов, экономия от переноса данных в облако может составлять до 35 % расходов на поддержание инфраструктуры². Однако при хранении и передаче данных в облаках могут возникнуть определенные угрозы, в частности неверная конфигурация, отсутствие стратегии облачной безопасности, слабое управление идентификацией, ключами и пр. Для защиты клиентских данных в облаке на примере Cloud³ предлагаются дополнительно законы, регулирующие вопросы безопасности облачной инфраструктуры, такие как Федеральный закон «О защите конкуренции», Федеральный закон «О связи» и пр. Таким образом, требования законодательства РФ к безопасности облачной инфраструктуры заключаются в обязанности операторов принимать меры по защите ПДн и КТ от несанкционированного доступа к ней и иных неправомерных действий.

¹ https://events.cnews.ru/articles/2023-03-29_dlya_perehoda_na_yuzedo_ne_hvataet

² <https://www.kommersant.ru/doc/5912890?query=cloud>

³ https://www.cnews.ru/reviews/security2022/cases/metody_zashchity_klientskih_dannyh?erid=Pb3XmBtz7ryKRhYZivkPYCgbcPTYWBmdmEQvgY

Часть 3. Существующие технологии и меры защиты

С учетом доступной аналитики многие проекты ЭДО обеспечивают полный контроль всех компонент собственной ИТ-инфраструктуры, которая создается, обновляется и управляется только собственными силами, без привлечения внешних консультантов, что обеспечивает дополнительную степень защиты чувствительной информации (прежде всего ПДн и КТ) и позволяют создать собственный «центр компетенции» по современным технологиям цифровой трансформации. Это подтверждается результатами работы в 2020–2023 гг. на международных конференциях: MSB, РКІ-Форум и «Комплексная защита информации».

Основной замысел проекта ЭДО был определен следующим образом:

- реализация интерфейса, который обеспечивает сервисы ЭДО для работников на едином доверенном и сертифицированном СКЗИ;
- реализация сервисов ЭДО на базе отечественной доверенной программной платформы «1С»;
- интеграция ИТ-инфраструктуры и сервисов ЭДО с существующими корпоративными решениями бухгалтерии, финансовых приложений и доверенных средств СЗИ/СКЗИ;
- обеспечение преемственности реализованного нормативно-методического базиса бухгалтерских (финансовых) приложений, учетных политик, нормативно-методических документов и требований ИБ;
- полная платформонезависимость и максимальная степень импортозамещения, все применяемые решения преимущественно произведены в РФ: платформы «1С:Бухгалтерия», «1С:ЭДО», 1С:Управление холдингом», СЗИ/СКЗИ и пр.

Основные задачи проекта ЭДО были определены как:

- перевод в электронный вид всех первичных учетных документов;
- развертывание собственного УЦ на базе национальных СКЗИ;
- развертывание инфраструктуры открытых ключей;
- выдача УКЭП руководителям Компании по стандартам ГОСТ;
- выдача НЭП работникам Компании по стандартам ГОСТ.

В процессе реализации проекта ЭДО удалось успешно решить еще одну проблему – устаревания нормативно-методической документации, которая регулирует вопросы обеспечения соответствия в области ИБ, безопасности ПДн, ЭДО и связанных ИТ-технологий. В частности, основные стандарты ISO и ISO/IEC (ГОСТ Р ИСО и ГОСТ Р ИСО/МЭК) периодически меняются и это было принято во внимание для обеспечения заданного уровня ИБ (*conformity assessment*) и соответствия (*compliance*). Например, заранее была получена информация о выходе одного из фундаментальных стандартов в области ИБ – ISO/IEC 27001 и введения нового ГОСТ Р ИСО/МЭК 27001–2021 в 2022 г.

Часть 4. Определение показателей доступности сервисов ЭДО

Нормативно-методические документы (ITIL, ISO, NIST, ГОСТ и пр.), обобщенно, разделяют проблему контроля нормального функционирования ИТ-сервисов на два направления – управление доступностью и управление непрерывностью. Первое направление – управление доступностью, кратко, характеризуется большим акцентом на проактивное управление и управление рисками. Второе направление – управление непрерывностью, кратко, больше ориентировано на реактивные меры с акцентом на минимизацию рисков. Краткое описание основных характеристик представлено далее.

Таблица 1. – Направления контроля функционирования ИТ-сервисов

Управление доступностью (AVA)	Управление непрерывностью (CONT)
Фокус на рисках с высокой вероятностью	Фокус на рисках с высоким ущербом (ЧС)
Больше проактивный	Больше реактивный

Снижает вероятность наступления нежелательных событий	Снижает ущерб от наступления нежелательных событий
Акцент на технических решениях	Акцент на организационных мерах
Оптимизация	Создание избыточности
Не является частью корпоративной функции	Является частью корпоративной функции
Business-as-usual	Форс-мажор
MTRS, MTBF (MTBSI)	RTO, RPO

Рассмотрим метрики, которые могут применяться при управлении доступностью:

– MTRS – среднее время восстановления услуги;
 – MTBF – среднее время между сбоями (от возобновления работы после сбоя до следующего сбоя);

– MTBSI – среднее время между инцидентами (от сбоя до следующего сбоя);

– RTO (recovery time objective) – целевое время восстановления после сбоя;

– RPO (recovery point objective) – целевая точка восстановления критических данных.

Рассмотрим примеры расчета доступности для двух наиболее характерных случаев:

– «Офисный» режим (8 рабочих часов с учетом часового перерыва, всего 9 часов 5 дней в неделю), всего 189 рабочих часов в месяц (при среднем количестве 21 рабочий день в месяц);

– «Непрерывный» режим (24 часа 7 дней в неделю), всего 720 рабочих часов в месяц (при среднем количестве 30 рабочих дней в месяц).

Примем во внимание, что в компании могут быть несколько ИТ-процессов с разными режимами работы, в том числе комбинированные.

Таблица 2. – Определение доступности для «офисного» режима

Показатель, %	95,00	98,00	99,00	99,90	99,99	99,999	99,9999	99,99999
Доступность	179,55	185,22	187,11	188,81	188,98	189,00	189,00	189,00
Простой (9×5), час	9,45	3,78	1,89	0,19	0,02	0,00	0,00	0,00
Простой (9×5), мин	567,00	226,80	113,40	11,34	1,13	0,11	0,01	0,00
Простой (9×5), с					68,04	6,80	0,68	0,07

Таблица 3. – Определение доступности для «непрерывного» режима

Показатель, %	95,00	98,00	99,00	99,90	99,99	99,999	99,9999	99,99999
Доступность	684,00	705,60	712,80	719,28	719,93	719,99	720,00	720,00
Простой (24×7), час	36,00	14,40	7,20	0,72	0,07	0,01	0,00	0,00
Простой (24×7), мин	2160,00	864,00	432,00	43,20	4,32	0,43	0,04	0,00
Простой (24×7), с					259,20	25,92	2,59	0,26

Графические примеры показаны далее.

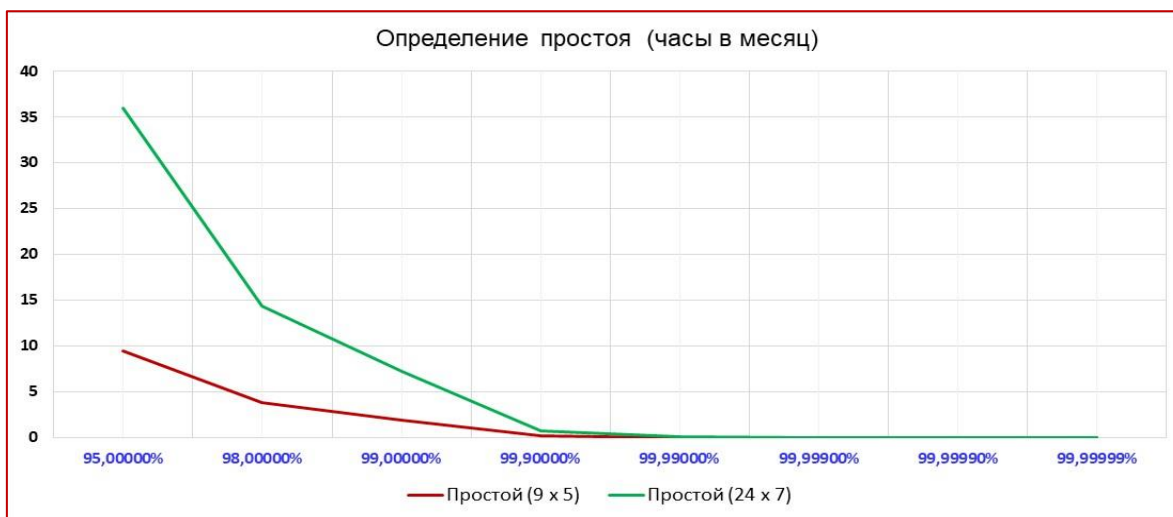


Рисунок 1. – Определение простоя (часы в месяц)

Очевидно, что для двух указанных режимов явно различимы значения допустимого простоя только до показателя доступности 99,0 % включительно. Если учесть норму регламентных работ минимум 1,89 часа в месяц, то нормальным показателем для «офисного» режима будет 98 %, а для «непрерывного» режима – 99,0 % соответственно. Обеспечить абсолютный результат 100 %, (без регламентных работ) практически возможно только для «офисного» режима, когда есть ночные часы и выходные дни, но невозможно при «непрерывном» режиме работы.

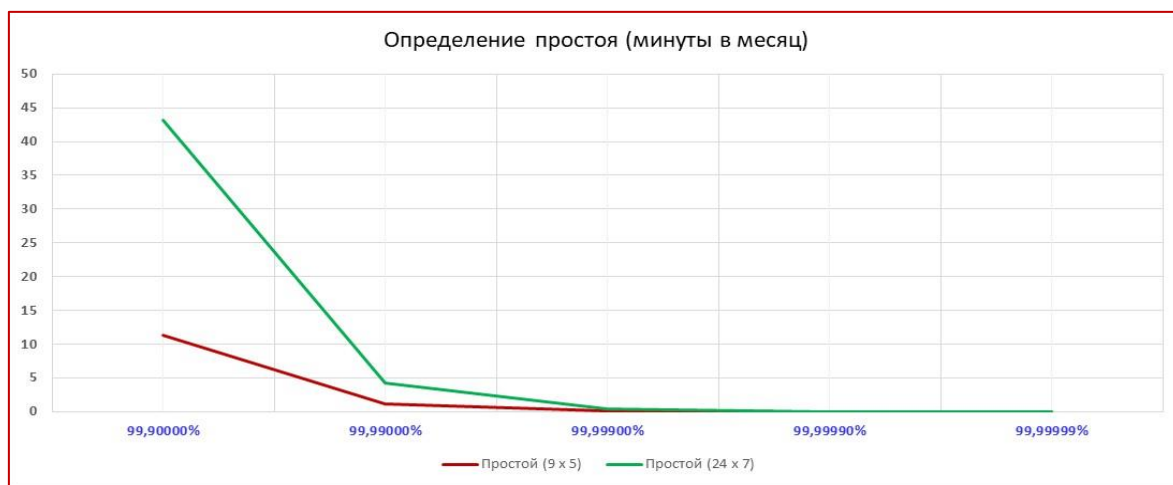


Рисунок 2. – Определение простоя (минуты в месяц)

Если увеличить масштаб и перейти к анализу показателя доступности в минутах, то становится очевидно, что уровень доступности 99,99 % можно обеспечить для «офисного» режима при простое 1,13 мин в месяц и для «непрерывного» режима при простое 4,32 мин в месяц соответственно. На практике вряд ли можно представить функционирование всех офисных приложений без наличия дополнительных (резервных) мощностей (офисное и серверное оборудование, каналы связи, доступные специалисты и лицензии ПО).

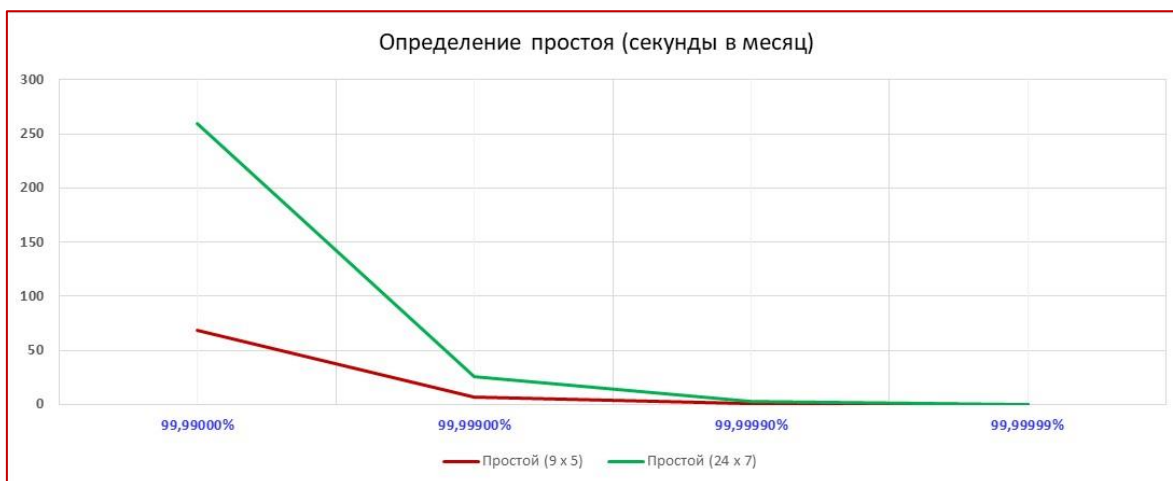


Рисунок 3. – Определение простоя (секунды в месяц)

Если увеличить масштаб и перейти к анализу показателя доступности в секундах, то становится очевидно, что уровень доступности 99,999 % можно теоретически обеспечить для «офисного» режима при простое 6,8 с в месяц и для «непрерывного» режима при простое 25,92 с в месяц, соответственно. На практике практически невозможно представить функционирование всех офисных приложений без наличия дополнительных (резервных) мощностей (офисное и серверное оборудование, каналы связи, доступные специалисты и лицензии ПО) с уровнем доступности выше 99,9 %. Достижение уровня доступности для «непрерывного» режима выше 99,99 % возможно только при существенном вкладе в дополнительные (резервные) мощности. Уровень доступности 99,999 % в настоящее время достижим только для специализированных ЦОД класса Tier III и выше, стоимость инфраструктуры которых может превышать сотни миллионов евро.

Недоступность сервисов в России

Рассмотрим несколько примеров недоступности известных ИТ-сервисов в РФ, по данным из открытых источников за последние 3 года.

– В 2019 г. известно о простое интернет-сервисов МТС, длительностью несколько часов.

– В 2020 г. известно о недоступности с 18 апреля более 14 часов сервисов Федеральной таможенной службы. Также известно о сбоях на сети «Ростелеком» 16.02.2020, длившихся несколько часов.

– В 2021 г. известно о недоступности в марте сервисов Яндекс, «Почта России» длительностью несколько часов. В сентябре известно о недоступности сервисов ФНС длительностью несколько часов. В ноябре несколько часов были недоступны сервисы «Госуслуги».

– В 2022 г. известно о продолжительных DDoS-атаках на «1С», в апреле сервисы были недоступны несколько дней. В мае известно о недоступности системы ЕГАИС (учета алкогольной продукции) в течение 2 дней из-за DDoS-атак.

На основании краткого анализа недоступности сервисов в России можно сделать вывод о том, что ни один из наиболее известных сервисов не гарантирован от простоев длительностью несколько часов минимум 1 раз в год. Соответственно, при «непрерывном» режиме работы этот показатель доступности можно оценивать в диапазоне 99,0–99,9 %, даже при условии более чем значительных вложениях в ИТ-инфраструктуру и сопутствующие сервисы на уровне федеральных бюджетов.

Нормативная база

Для определения доступности как одной из составляющей надежности систем в РФ может выполняться по разным нормативным документам, например:

1. ГОСТ Р 27.013-2019 Методы оценки показателей безотказности (перевод ИЕС 62308:2006 "Equipment reliability – Reliability assessment methods", MOD).
2. ГОСТ РВ 51987-2002 «Информационная технология. Комплекс стандартов на АС. Типовые требования и показатели качества функционирования информационных систем».

Выводы

1. Для обеспечения доступности сервисов ЭДО в собственной ИТ-инфраструктуре предлагается ориентироваться на выбор стратегии принятия тех рисков, передача и/или обработка которых экономически нецелесообразна.
2. При невозможности обеспечения абсолютного (минимальное приемлемого) уровня доступности системы ЭДО (в равной степени – внешних компонент) необходимо использовать собственную ИТ-инфраструктуру.
3. В своей ИТ-инфраструктуре необходимо контролировать все стадии жизненного цикла системы ЭДО (проектирование, развертывание и сопровождение в собственном полностью контролируемом периметре).
4. На практическом проекте в собственной ИТ-инфраструктуре решение ЭДО обеспечило в 2022 г. результаты доступности 99,965 % (чуть больше 3 часов в год, примерно 15 минут в месяц).

Литература

1. Лившиц И.И., Соколов Е.О., Лукьянова А.А. Схемотехнические решения для практической реализации безопасного электронного документооборота. Часть 2. Новая разработка / Газовая промышленность, 2022. – № 11 (840)
2. Лившиц И.И., Соколов Е.О., Лукьянова А.А. Схемотехнические решения для практической реализации безопасного электронного документооборота. Часть 1. Аналитический обзор / Газовая промышленность, 2022. – № 9 (837). – С. 40–56.
3. Лившиц И.И., Соколов Е.О., Лукьянова А.А. Расчет экономического эффекта для проекта кадрового электронного документооборота // Стандарты и качество, 2022. – № 12. – С. 67–74.

Грантовая программа

Проект реализуется победителем грантового конкурса для преподавателей магистратуры 2022/2023 г. Стипендиальной программы Владимира Потанина

Авторы

Лившиц Илья Иосифович, д.т.н., профессор факультета ФБИТ, Университет ИТМО.

Адрес для корреспонденции

197101, Российская Федерация,
Кронверкский пр., д. 49, лит. А, Санкт-Петербург,
Федеральное государственное автономное образовательное учреждение высшего
образования «Национальный исследовательский университет ИТМО»
(Университет ИТМО)
+7 (921) 934-48-46
Email: Livshitz.il@yandex.ru
Лившиц Илья Иосифович

ОСНОВНЫЕ МЕХАНИЗМЫ ФОРМИРОВАНИЯ И ИСПОЛЬЗОВАНИЯ ЭФФЕКТА «ВИРТУАЛЬНОЙ ТОЛПЫ» ПРИ РЕШЕНИИ ЗАДАЧ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

С.П. ЛАРИН, А.Н. НАСЕВИЧ

*Государственное учреждение «Научно-исследовательский институт Вооруженных Сил
Республики Беларусь», г. Минск, Республика Беларусь*

Введение

В настоящее время социальная и политическая ситуация в Республике Беларусь и в других странах такова, что структуры власти не могут опираться только на силовые методы управления массовым поведением людей. Реальные события, их последствия и подаваемая интерпретация в средствах массовой коммуникации (СМК) непосредственно влияют на сознание, мотивацию и поведение общества (психическая травматизация участников событий, посттравматическое стрессовое расстройство и острые стрессовые реакции). В настоящее время СМК выступают посредниками общения между людьми и становятся инструментами построения образа действительности наряду с личным опытом и межличностным взаимодействием, формируя и трансформируя их представления. Катализатором общественных процессов стал Интернет, который, создав новую информационную среду, привел к появлению новых моделей взаимодействия не только членов общества между собой, а также общества и государства, но и других субъектов, оказывающих деструктивные воздействия. При достаточно целенаправленном, длительном и непрерывном процессе часть общества (в силу различных причин) оказывается в таком психоэмоциональном состоянии, что может совершать действия, противоречащие ее интересам. В результате возникает «эффект толпы», который формирует общности людей, обладающих своими отличительными признаками (свойствами) и осуществляющих свою деятельность неосознанно, реализуя цель (цели) субъекта информационного противоборства (ИПб).

Механизмы манипулирования массовым сознанием

В основных документах США, определяющих основные направления развития оперативно-стратегических концепций применения вооруженных сил в XXI веке, подчеркивалось, что главной чертой вооруженной борьбы будет перенос акцента в сферу информационного противоборства и достижение информационного господства станет обязательным условием победы над любым противником. При этом для повышения эффективности информационно-психологических воздействий (ИПВ), как правило, используются научные разработки в области социальной психологии, лингвистики, управления массовым и индивидуальным сознанием. Многие отечественные и зарубежные исследователи в области социальной психологии, политологии, массовой коммуникации и управления подтверждают использование интернет-технологий для воздействия на большие социальные группы, минуя контроль властных структур [1–3]. Примерами практической реализации такого воздействия на массовое сознание и поведение различных групп населения являются так называемые цветные революции, где основной упор осуществлялся на выявлении особенностей (характеристик) каждой социальной группы страны-жертвы с позиции определения ее «уязвимостей» для максимизации эффекта ИПВ.

Известно [4, 5], любое общество можно стратифицировать в отношении больших социальных групп (БСГ), т.е. групп, сложившихся в ходе исторического развития общества, занимающие определенное место в системе общественных отношений каждого конкретного типа общества, и потому долговременные, устойчивые в своем существовании. К ним относят, прежде всего, социальные классы, различные этнические группы (как их главную разновидность – нации, народности), профессиональные группы, половозрастные группы. С этой точки зрения в качестве БСГ могут быть рассмотрены, например, молодежь,

трудоспособное население, пенсионеры и т.д. Исходя из свойств данных групп «пошатнуть» их в отношении принуждения к определенному типу поведения крайне сложно, практически невозможно, поэтому необходим целенаправленный процесс по изменению ценностных ориентиров, что в итоге может привести к «расчеловечиванию» общества, превращая часть этого общества в нестабильные, неустойчивые образования, – толпу. Поскольку к неустойчивым (стихийным) образованиям относят также публику (аудиторию) и массу, следует дать определения каждому из данных явлений [4].

Публика – это собрание людей для совместного времяпрепровождения в связи с каким-то зрелищем – на трибуне стадиона, в большом зрительном зале. Публика всегда собирается ради общей и определенной цели, поэтому она более управляема, в частности в большей степени соблюдает нормы, принятые в избранном типе организации зрелищ.

Масса обычно описывается как довольно стабильное образование с нечеткими границами. Как правило, понятие масса применяется тогда, когда определенные слои населения достаточно сознательно собираются ради какой-либо акции: манифестации, демонстрации, митинга. В действиях массы продуманы как конечные цели, так и тактика поведения. Вместе с тем, масса достаточно разнородна, в ней могут сосуществовать, так и сталкиваться различные интересы, поэтому ее состояние может быть неустойчивым.

Толпа образуется по поводу самых различных событий, длительность ее существования определяется значимостью инцидента. В другом случае, особенно когда это связано с выражением недовольства каким-либо социальным явлением эмоциональный накал толпы может возрасти, порождая агрессивное поведение участников, в толпе могут возникать элементы организации, если находится человек, который сумеет ее возглавить. Но если даже такие элементы возникли, они очень нестабильны: толпа легко может и смести возникшую организованность. Стихия остается основным фоном поведения толпы, приводя часто к ее агрессивным формам.

Зачастую отдельные категории массовых явлений могут переходить из одной в другую, например, публика на стадионе (болельщики футбола) вследствие какого-либо инцидента, может стать неуправляемой толпой, где действуют свои законы поведения.

Учитывая классические представления о «психологии толпы», необходимо переосмыслить особенности массового сознания и поведения больших социальных групп в связи с возможностями реализации различного вида информационных воздействий на основе использования современных интернет-технологий, которые позволяют осуществлять информационный обмен без ограничений по времени, территориальному размещению, тематике распространяемых сведений. Это позволяет субъектам управления осуществлять воздействие на общественное сознание скрытно, стирая индивидуальность каждого индивида, заменяя ее обезличенной (фиктивной) формой самопрезентации в различных сетевых ресурсах.

В результате интернет-пространство превращается в многочисленные фиктивные сообщества, в которых эмоции каждого его члена имеют тенденцию выражаться спонтанно, а большое количество и темпы передачи информации ведут к информационной зависимости того или иного виртуального сообщества. Проведенный анализ событий, приведших к дестабилизации общества в Украине (2013–2014 гг.), Беларуси (2020 г.), России (2021 г.), проявившихся в массовых несанкционированных демонстрациях, митингах, пикетах и т.д., позволил выявить механизмы формирования протестного потенциала посредством использования информационных технологий, при этом основным элементом данного процесса являлось создание эмоционально заряженной «виртуальной массы». Полученные выводы, с учетом основных положений социальной психологии, подтверждают, что данному виртуальному образованию («виртуальной массе») присущи свойства обычной толпы, такие как заражаемость, внушаемость и подражаемость [4].

Заражаемость. В самом общем виде эффект заражения можно определить, как бессознательную невольную подверженность индивида определенным психическим состояниям. Поскольку это эмоциональное состояние возникает в массе, действует механизм многократного взаимного усиления эмоциональных воздействий общающихся людей.

Индивид здесь не испытывает организованного преднамеренного давления, но просто бессознательно усваивает образцы чьего-то поведения, лишь подчиняясь ему. Многие исследователи констатируют наличие особой «реакции заражения», возникающей особенно в больших открытых аудиториях, когда эмоциональное состояние усиливается путем многократного отражения по моделям обычной цепной реакции. Эффект имеет место прежде всего в неорганизованной общности, чаще всего в толпе, выступающей своеобразным ускорителем, который «разгоняет» определенное эмоциональное состояние.

Внушаемость представляет собой свойство, вызываемое целенаправленным, неаргументированным воздействием одного человека на другого или на группу. При внушении осуществляется процесс передачи информации, основанный на ее некритическом восприятии.

Подражаемость – обусловленное копированием поведения других людей, в том числе в условиях массового поведения, не имея собственной, внутренней устойчивой позиции. Эффект подражания имеет ряд общих черт с уже рассмотренными явлениями заражения и внушения, однако его специфика состоит в том, что здесь осуществляется не простое принятие внешних черт поведения другого человека или массовых психических состояний, но воспроизведение индивидом черт и образцов демонстрируемого поведения.

Для усиления способов (механизмов) воздействия, приводящие к вышеизложенным эффектам, администраторы, модераторы и прочие агенты влияния путем использования различных способов подачи информации, негативно/позитивно окрашенной лексики, фотографического материала, стилистических приемов, сокрытия нежелательных для публикации тем в форме общения в виртуальных сетях создают необходимый когнитивный эффект. При этом для повышения эффективности вовлечения людей в социальные сети используются следующие основные виды мотиваций [1]: чувство справедливости; вера в роль большинства; желание поддержать или выступить против конкретной проблемы и др.

Наглядным примером применения технологий формирования виртуальной массы с последующим превращением ее в толпу стали события на Украине в 2004 и 2014 гг. С обретением данной страной «независимости» вследствие развала СССР в 1991 г., приоритетной задачей информационной кампании коллективного Запада являлась отрыв Украины от России и «переформатирование» граждан Украины, что они «не такие, как там». Важнейшим инструментом этого процесса является так называемая оранжевая сеть, которая была создана по всем правилам ведения «сетевых операций» [3], посредством которой на Украине было наглядное формирование систем поведения всех сторон, начиная от президентов (Кравчука, Кучмы, Ющенко, Януковича, Порошенко, Зеленского), элит, масс, политтехнологов, экономических кланов, высших чиновников, заканчивая социальными группами.

Аналогичные механизмы формирования «виртуальной массы» применялись в нашей стране в 2020 г. перед выборами Президента Республики Беларусь. В интересах дестабилизации общества были использованы возможности ТГ-каналов, которые стали ключевым инструментом освещения политических процессов, в том числе средством управления социальными группами практически в режиме реального времени. На платформе «Телеграмм» западные структуры выстраивали свои самые современные и эффективные, так называемые сетевые модели управления, эффективно противостоять которым даже в настоящее время достаточно сложно.

Анализ данного процесса показал наличие отработанного механизма оказания ИПВ посредством специально подобранного, красочного, информативного и эмоционально заряженного (обязательное условие) контента, манипулирования общественным мнением через так называемых агентов влияния, подставных лиц, «троллей». Данная технология позволила в кратчайшие сроки сформировать «виртуальную массу», которая впоследствии была мотивирована на массовые несанкционированные действия (демонстрации, митинги, шествия и т.п.) для нужных для субъектов управления месте и времени.

Ставка режиссеров «оранжевых революций» делается на молодежь. Выбор в качестве объекта воздействия данной социальной группы объясняется тем, что она в большей степени

склонна ко всему новому, перспективному, где развиты групповые коммуникации и приверженность идеи в объединении с Западом как решение всех своих проблем, именно эта социальная группа выступает главным объектом современных глобальных манипуляций. В силу того, что молодежь не обладает достаточным социальным опытом, отличается доверчивостью и неискушенностью в политике, более склонна верить в «светлое», «национальное», «демократическое» будущее, менее интегрирована в политические структуры, относительно слабо задействована в институтах власти, способна на необдуманные, рискованные и даже авантюристические действия она в большей степени манипулируема, чем остальные социальные группы.

При толпообразовании начинается процесс идентификации по принципу «МЫ и ОНИ». Резко возрастает групповая солидарность, одновременно резко повышается негативизм оппонентов. Последнее особенно ярко проявилось в бывшей Югославии, где люди на протяжении веков, жившие в одном селе, вдруг оказались по разные стороны баррикад. Такая же ситуация характерна и для современной Украины, где даже в одной семье родители общаются предпочтительно на русском, а дети – на украинском. Если в обычной действительности есть определенные «охлаждающие процедуры», которые не дают довести данное напряжение до насильственных действий, то в рамках ПсО их сознательно или случайно начинают блокировать. Можно назвать следующие моменты «остановки», которые пытаются обойти [1]:

время (создается ощущение срочности, необходимости немедленного решения проблемы);
отсутствие опыта (никто не знает, к каким последствиям все это может привести, поскольку прогнозируют ситуацию исходя из норм поведения, принятых в обычной ситуации);
защитное влияние толпы (человек в толпе ощущает себя частью целого, а не индивидуумом: «я – как все»);

вербальные объединители снимают, блокируют индивидуальные реакции, не позволяя выделиться со своей собственной реакцией на происходящее. При радикализации виртуальной толпы вводятся фразы типа «клянемся!», «Слава героям – героям слава!». Толпа становится единым целым благодаря единству реакций, которые проявляются в двух-трех типах фраз, которые могут выступать как маркеры для опознавания «свой-чужой» («кто не скаче, той москаль», «москаляку на гиляку» ...).

Следует понять, что современные ПсО несут в себе более серьезный интеллектуальный компонент (чем это было ранее) за счет использования современных методов управления массами и информационных технологий. Поэтому высокоразвитые страны будут иметь постоянное преимущество, уровня которого будет достаточно сложно достигнуть. Нельзя будет даже понять, что начавшиеся информационно-психологические воздействия не случайны, а носят системный и планомерный характер. В данных условиях реакция на данные воздействия может оказаться запоздалой и неэффективной, а результаты – крайне негативные, о чем свидетельствует опыт ряда стран, в особенности – Украины.

Заключение

1. Эффективность ИПВ в ходе «цветных революций» в большей степени обусловлена широким распространением информационно-телекоммуникационных технологий и активным вовлечением граждан в социальные сети. Это позволяло вести массированную адресную пропаганду без существенных финансовых затрат, оценивать ее эффективность, вносить коррективы в процесс в реальном масштабе времени. Как показывают украинские события, с помощью манипулирования государственными СМИ и социальными сетями возможно конструировать «альтернативные реальности», радикально отличающиеся, а иногда противоречащие объективной действительности.

2. Особенностью современного общества является процесс его информатизации. Если раньше для общения больших масс людей необходимо было физическое их присутствие в одном месте, то современные информационные технологии позволяют это сделать «виртуально», где создается «эффект присутствия». Однако при целенаправленном и продолжительном воздействии из аудитории можно сделать «виртуальную массу», которой

присущи классические свойства обычной толпы. А когда она окажется на улице и какова будет модель поведения – это только вопрос времени и особенностей ИПВ.

3. С учетом складывающейся политической обстановки в мире нельзя исключать возможность инициации «цветной революции» как в Российской Федерации, так и в Республике Беларусь. При этом могут быть применены еще более агрессивные и изощренные способы дестабилизации общества. В этих условиях только понимание и наличие соответствующей технологии противодействия (включая не только защиту, но и нападение) современным ПсО может дать положительный эффект. Однако, на наш взгляд, не осознав в полной мере механизм толпообразования посредством интернет-технологий и не актуализировав вопрос о мониторинге информационного контента в социальных сетях и СМК, создать и эффективно использовать такую технологию проблематично.

Литература

1. Почепцов, Г.Г. Информационные войны. М.: Рефл-бук, 2000. – 576 с.
2. Федорова, А.А. Сетевые репрезентации этнонациональных групп в виртуальном пространстве русской этничности: дис. ... канд. соц. наук: 23.00.06 / А.А. Федорова. – СПб, 2019. – 343 л.
3. Нарочницкая, Н. А. Оранжевые сети от Белграда до Бишкека // Фонд исторической перспективы. – СПб.: Издательство «Алетейя», 2008 г.
4. Андреева, Г.М. Социальная психология. Учебник для высших учебных заведений. – М.: Аспект Пресс, 2001.
5. Лашук, И.В. Социокультурный анализ современного белорусского общества / И.В. Лашук // Ин-т социологии Нац. акад. наук Беларуси. – Мн: Бел. навука, 2019. – 267 с.

ПЛАНИРОВАНИЕ ЦЕЛЕВОГО ПРИМЕНЕНИЯ БОЛЬШИХ КЛАСТЕРОВ МАЛЫХ КОСМИЧЕСКИХ АППАРАТОВ В УСЛОВИЯХ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ

А.Н. КОРОЛЕВ, Г.В. КОРОВИН

*«НИИ КС имени А.А. Максимова» – филиал АО «ГКНПЦ им. М.В. Хруничева»,
г. Королев, Российская Федерация*

Введение

Одним из наиболее перспективных направлений развития будущих орбитальных группировок автоматических космических аппаратов (КА) является их структурное построение в виде кластеров. При этом под кластером понимается совокупность разнотипных КА, решающих совместно одну целевую задачу и с точки зрения потребителя являющихся одним КА [1].

При построении кластера КА наиболее трудоемкой в вычислительном плане является задача распределения частей целевой функции между членами «роя», таким образом, чтобы обеспечить максимум качества выполнения целевой задачи кластером в целом. Кластер в процессе своего функционирования подвергается различного рода деструктивным воздействиям, которые вызывают изменение технического состояния входящих в него КА и системы межспутникового информационного обмена, что ведет к деградации функциональных возможностей кластера по реализации целевой функции.

В настоящее время наиболее перспективным подходом к целевому планированию большеразмерного кластера КА типа «распределенный космический аппарат» является планирование на основе функционально-распределенных вычислений. В соответствии с [1] такой кластер состоит из множества однотипных КА одинаковой размерности («фемто», «пико» или «нано») и, одного (или нескольких) специализированного КА большей, по сравнению с остальными, размерности, осуществляющего управление кластером и информационный обмен с наземной инфраструктурой – орбитальный центр обработки данных (ЦОД). ЦОД получает целевую задачу с наземного комплекса управления и организует распределение целеуказаний между КА кластера.

1. Задача распределения целеуказаний в кластере КА и подход к ее решению на основе функционально-распределенных вычислений

Рассмотрим целевую задачу Q , которая для кластера КА может быть представлена набором целевых эффектов [2] $Q = \{Q_i\}, i = 1, N$, при этом каждый целевой эффект (ЦЭ) характеризуется набором параметров, которые должны быть выполнены при его реализации. Например, для кластера видового зондирования помимо интервала времени съемки и координат изображения указываются требуемые параметры съемки: разрешающая способность (обзорная, детальная, высокодетальная), спектральная чувствительность (панхроматическая, многоспектральная, гиперспектральная) и т.д. Для ЦЭ в рамках решения целевой рассматривается несколько уровней параметров, что позволяет сформировать для каждого ЦЭ частично упорядоченное множество

$$Q_i = \{q_j^i\}, j = \overline{0, L_i}, \forall (q_k^i, q_m^i, k > m) \Rightarrow q_k^i \geq q_m^i,$$

где каждый элемент множества q_j^i имеет свой набор параметров, который соответствует реализации ЦЭ Q_i с определенным уровнем качества, при этом $q_{L_i}^i$ – максимально возможный уровень качества реализации i -го ЦЭ, q_0^i – неприемлемо низкий уровень качества или отсутствие возможности реализации ЦЭ.

Отсюда целевая задача, передаваемая кластеру в общем виде представляет собой массив данных в виде квазиматрицы (матрицы с разными длинами строк)

$$Q^* = \left\| \begin{array}{ccc} q_0^1 & \dots & q_{L_1}^1 \\ \vdots & \ddots & \vdots \\ q_0^N & \dots & q_{L_N}^N \end{array} \right\| = \|q_j^i\|, i = \overline{1, N}, j = \overline{0, L_i}.$$

На Q^* определяется множество векторов

$$A = \{\mathbf{a}_j\}, \mathbf{a}_j = \langle q_{i_1}^1, q_{i_2}^2, \dots, q_{i_N}^N \rangle, i_k = \overline{0, L_k}, k = \overline{1, N}, j = 1, \prod_{i=1}^N L_i,$$

где каждый вектор \mathbf{a}_j соответствует определенному уровню качества реализации целевой задачи Q .

На множестве векторов A вводится частичный порядок, такой, что для любых двух векторов \mathbf{a}_i и \mathbf{a}_j вектор \mathbf{a}_i предпочтительнее \mathbf{a}_j , если для каждого ЦЭ Q_l из набора Q качество реализации $q_{k_l}^l$, принадлежащее вектору \mathbf{a}_i , не хуже качества реализации этого ЦЭ $q_{m_l}^l$, принадлежащего вектору \mathbf{a}_j

$$\mathbf{a}_i \succcurlyeq \mathbf{a}_j: \forall (q_{k_l}^l \in \mathbf{a}_i, q_{m_l}^l \in \mathbf{a}_j, l = \overline{1, N}) (k_l \geq m_l),$$

и метрика, определяющая расстояние между двумя векторами на множестве A как

$$d(\mathbf{a}_i, \mathbf{a}_j) = \sqrt{\sum_l (k_l - m_l)^2}, q_{k_l}^l \in \mathbf{a}_i, q_{m_l}^l \in \mathbf{a}_j, l = \overline{1, N}.$$

Каждый КА кластера (включая ЦОД, если на нем размещена целевая аппаратура) с точки зрения целевой задачи представляет собой элементарный ресурс z_i , который может использоваться для реализации одного или более ЦЭ из набора Q , но не более, чем для реализации одного ЦЭ на заданном интервале времени. Если техническое состояние КА на заданном интервале времени позволяет реализовывать несколько ЦЭ, то он рассматривается как набор элементарных ресурсов.

Функционально-распределенные вычисления для управления кластером реализуются по схеме многоагентной системы на основе модели «Запрос – Ответ – Соглашение» [3]. ЦОД, получив целевую задачу Q , транслирует ее в виде запроса всем КА кластера. Каждый КА кластера на основе имеющейся у него информации о параметрах своего движения, наличии и работоспособности целевой аппаратуры, энергоресурсах и др. оценивает свои возможности по реализации целевых эффектов задачи. В ЦОД в виде ответа каждый КА представляет по каждому своему элементарному ресурсу z_m матрицу своих функциональных возможностей по решению целевой задачи

$$S(z_m) = \left\| \begin{array}{ccc} s_0^1 & \dots & s_{L_1}^1 \\ \vdots & \ddots & \vdots \\ s_0^N & \dots & s_{L_N}^N \end{array} \right\| = \|s_j^i\|, i = \overline{1, N}, j = \overline{0, L_i},$$

где $s_j^i = \begin{cases} 1, & \text{если КА способен реализовать } i - \text{й ЦЭ на уровне качества } q_j^i; \\ 0, & \text{в противном случае.} \end{cases}$

Далее ЦОД, получив данные от всех M_r работоспособных элементарных ресурсов кластера, готовит соглашение, для чего формирует матрицу функциональных возможностей кластера по решению целевой задачи на уровне качества \mathbf{a}_k (первоначально обычно $\mathbf{a}_k = \mathbf{a}_{max}$) размерности $M_r \times N$ следующего вида:

$$B(\mathbf{a}_k) = \begin{bmatrix} b_{1,1} & \cdots & b_{1,N} \\ \vdots & \ddots & \vdots \\ b_{M_r,1} & \cdots & b_{M_r,N} \end{bmatrix}, b_{i,j} = s_{k_j}^j, s_{k_j}^j \in S(z_i).$$

Для того чтобы распределить ЦЭ по элементарным ресурсам необходимо построить инъективное отображение из конечного множества ЦЭ мощности N в конечное множество элементарных ресурсов мощности M_r , $M_r \geq N$, при котором каждому индексу e ЦЭ Q_e из первого множества ставится в соответствие индекс $\sigma(e)$ элементарного ресурса $z_{\sigma(e)}$ из второго множества. Обычно это соответствие записывается в виде матрицы [4]

$$\begin{pmatrix} 1 & 2 & \dots & N \\ \sigma(1) & \sigma(2) & \dots & \sigma(N) \end{pmatrix}.$$

Последовательность $(b_{\sigma(1),1}, b_{\sigma(2),2}, \dots, b_{\sigma(N),N})$ называется диагональю, а произведение $b_{\sigma(1),1} b_{\sigma(2),2} \dots b_{\sigma(N),N}$ – диагональным произведением длины N матрицы B размерности $M_r \times N$, $M_r \geq N$.

2. Общая схема и алгоритмы решения задачи распределения целеуказаний в кластере КА

Целевая задача реализуема кластером на уровне качества \mathbf{a}_* в случае, если каждый j -й ЦЭ из набора Q реализуется на отдельном элементарном ресурсе z_i , причем этот ресурс имеет возможность реализовать его на уровне качества $q_{k_j}^j \in \mathbf{a}_*$. Другими словами, матрица B должна содержать хотя бы одно ненулевое диагональное произведение длины N .

Таким образом, формирование соглашения (решение задачи целевого планирования) сводится к двухэтапной схеме:

1. Находится допустимый максимальный вектор качества решения целевой задачи \mathbf{a}_* , при котором существует распределение всех ЦЭ по имеющимся работоспособным элементарным ресурсам кластера путем формирования матрицы $B(\mathbf{a}_*)$ и проверки наличия в ней хотя бы одного ненулевого диагонального произведения длины N .

2. Находится допустимое распределение ЦЭ по элементарным ресурсам σ путем определения положительной диагонали $(b_{\sigma(1),1}, b_{\sigma(2),2}, \dots, b_{\sigma(N),N})$ в матрице $B(\mathbf{a}_*)$.

На основании сформированного соглашения ЦОД передает целеуказание космическим аппаратам кластера по решению целевой задачи, то есть каждому из N элементарных ресурсов кластера $z_{\sigma(i)}$ назначается i -й ЦЭ для реализации на уровне качества $q_{k_i}^i \in \mathbf{a}_*$.

Алгоритм определения допустимого максимального вектора качества решения целевой задачи \mathbf{a}_* при наборе из M_r работоспособных элементарных ресурсов кластера строится на основе анализа числовой матричной функции – перманента бинарной матрицы $B(\mathbf{a}_*)$ [4]. Перманент матрицы $\text{Per } A$ матрицы A размерности $m \times n$, $m \geq n$ есть числовая функция, определяемая как сумма всех ее диагональных произведений

$$\text{Per } A = \sum_{\sigma} \prod_{i=1}^n a_{i,\sigma_i}.$$

Перманент квадратной матрицы, так же, как и определитель, может быть вычислен с помощью разложения Лапласа по элементам строк, но, в отличие от определителя, суммирование ведется без учета знаков алгебраических дополнений миноров. Перманент является знакопостоянной функцией и, в отличие от определителя, может быть вычислен для прямоугольной матрицы. В этом случае он может вычисляться как сумма всех перманентов максимальных квадратных матриц прямоугольной матрицы.

В [5] доказано: для того, чтобы система, имеющая в составе набор из M_r работоспособных элементарных ресурсов, больший или равный количеству элементарных функций, обеспечивающих реализацию целевой задачи на уровне качества \mathbf{a}_* , необходимо и достаточно, чтобы перманент матрицы $B(\mathbf{a}_*)$ был положителен $\text{Per } B(\mathbf{a}_*) > 0$. Там же сформулировано и доказано утверждение, что если в бинарной матрице размерности $m \times n$, $m \geq n$ минимальное количество строк или столбцов, сумма элементов которых больше нуля, больше или равно n , то ее перманент больше нуля.

На основании вышеприведенных утверждений можно построить алгоритм, который позволит за приемлемое время определить допустимый вектор уровней качества выполнения целевой задачи, близкий к максимально возможному [5].

Для определения допустимого распределения ЦЭ по матрице $B(\mathbf{a}_*)$ проводят разложение ее перманента по правилам, аналогичным разложению Лапласа для определителя матрицы, но без учета знаков. В отличие от определителя матрицы разложение перманента относится к классу задач еще более сложных, чем NP полные, поэтому прямой поиск ненулевой диагонали, как правило неприемлем для больших матриц. В [5] показано, что если построить алгоритм поиска допустимого распределения на основе рекуррентной процедуры последовательного выбора ненулевых элементов, находящихся на пересечении строк и столбцов матрицы (подматрицы), содержащих минимальное количество единиц, то асимптотическая оценка скорости нахождения нужной перестановки оценивается как $O(M_r)$.

Однако, рассмотренный алгоритм корректно работает в случае, если каждый элементарный ресурс кластера правильно диагностирует свое техническое состояние и параметры движения. Если же вследствие деструктивных воздействий на кластер, выражающихся в недостоверной работе подсистемы контроля технического состояния КА или несанкционированном вмешательстве извне в управление КА или функционирование системы межспутникового обмена, ЦОД получит неверные данные о функциональных возможностях КА по решению целевой задачи, то это может привести к некорректному распределению ЦЭ между ресурсами кластера, что, в свою очередь, приведет к снижению качества реализации целевой функции вплоть до срыва выполнения целевой задачи кластером.

Для парирования подобной ситуации целесообразно в процесс формирования соглашения (решение задачи целевого планирования) вводится модель доверия информации о функциональных возможностях КА. Модель формируется следующим образом. Для каждого элементарного ресурса кластера z_m назначается коэффициент доверия $\mu(z_m) \in [0,1]$. Первоначально для всех элементарных ресурсов $\mu(z_m) = 1$. Далее после обработки наземными средствами результатов решения очередной целевой задачи на ЦОД отправляются данные о фактическом уровне качества каждого i -го ЦЭ \tilde{q}_j^i , полученным при реализации его назначенным элементарным ресурсом КА $z_{\sigma(i)}$. ЦОД сравнивает фактический уровень качества реализации ЦЭ \tilde{q}_j^i с уровнем качества \mathbf{a}_* , на котором проводилось планирование решения целевой задачи. Если $\tilde{q}_j^i \neq q_j^i \in \mathbf{a}_*$, то для ресурса z_m его коэффициент доверия $\mu(z_m)$ снижается, в противном случае повышается. Теперь при следующем планировании распределения ЦЭ по элементарным ресурсам алгоритм поиска допустимого распределения строится на основе рекуррентной процедуры последовательного выбора ненулевых элементов матрицы $B(\mathbf{a}_*)$, находящихся на пересечении строк, соответствующих элементарным ресурсам с максимальным коэффициентом доверия, и столбцов матрицы (подматрицы), содержащих минимальное количество единиц [5]. Такой подход позволяет максимально снизить влияние недостоверной информации о функциональных возможностях элементарных ресурсов при решении задачи распределения ЦЭ между ними.

Поскольку суммарная сложность рассматриваемых алгоритмов может оцениваться как $O(N \times M_r)$, то задачу планирования целеуказания для кластера КА можно отнести к классу «хорошо решаемых», что в принципе позволяет решать ее бортовыми вычислительными средствами даже для кластеров, содержащих тысячи элементарных ресурсов.

Заключение

1. Задача планирования целевого применения большеразмерных кластеров КА, функционирующих в условиях деструктивных воздействий, может быть решена на основе функционально-распределенных вычислений на КА, являющихся элементами кластера, с использованием принципов построения многоагентных систем.

2. Поиск допустимого распределения целеуказаний в кластере КА осуществляется по двухэтапной схеме. На первом этапе находится вектор допустимый вектор качества решения целевой задачи, который способен обеспечить кластер КА в его текущем техническом состоянии, на основе которого формируется матрица функциональных возможностей кластера КА. На втором этапе по этой матрице определяется допустимое распределение целевых эффектов между элементарными ресурсами кластера.

3. Для снижения негативного воздействия недостоверной информации о функциональных возможностях элементарных ресурсов КА на принятие решения по распределению целевых эффектов алгоритм поиска допустимого распределения должен быть скорректирован с учетом модели доверия к этой информации.

Литература

1. Ключников В.Ю. Построение кластеров малых космических аппаратов // Изв. вузов. Приборостроение, 2016. – Т. 59, № 6. – С. 423–428.

2. Волков С.А. К постановке задачи управления многоспутниковыми орбитальными группировками / С.А. Волков, А.Ю. Потюпки, Ю.А. Тимофеев. – Научное значение трудов К.Э. Циолковского: история и современность. Материалы 55-х Научных чтений памяти К.Э. Циолковского. – Калуга: Издательство «Эйдос», 2020. – С. 61–64.

3. Многоагентная система // Википедия: [сайт]. – 2021, URL: https://ru.wikipedia.org/wiki/Многоагентная_система (дата обращения: 09.05.2022).

4. Тараканов В. Е. Комбинаторные задачи и $(0,1)$ – матрицы / В.Е. Тараканов. – М.: Наука. Гл. ред. физ.-мат. лит., 1985. – 192 с.

5. Королев А.Н. Функциональная устойчивость навигационно-информационных систем: монография / А.Н. Королев. – М.: Издательство «Триумф», 2022. – 192 с.

О МЕТОДОЛОГИЧЕСКОЙ ПРОБЛЕМЕ, ПРЕПЯТСТВУЮЩЕЙ ВНЕДРЕНИЮ СТРАХОВАНИЯ ИНФОРМАЦИОННЫХ РИСКОВ В ПРОЦЕССЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

В.А. ВОЕВОДИН

*Национальный исследовательский университет «МИЭТ»,
г. Зеленоград, Российская Федерация*

Введение

Страхование информационных рисков физических и юридических лиц в развитых странах позиционируется как экономический инструмент управления информационной безопасностью. Первый полис киберстрахования (известный как Полис ответственности за безопасность в Интернете) появился в страховой отрасли и в бизнесе в 1997 г. В конце 2000-х гг. на зарубежном европейском рынке началось расширение охвата рынка услуг страхования информационных рисков. Существуют прогнозы, что к 2025 г. рынок страхования рисков информационной безопасности в Европе достигнет 21,4 млрд долларов [1]. Это связано, прежде всего с тем, что быстрый рост социальной инженерии и широкого спектра вредоносных программ, особенно программ-вымогателей, резко увеличил вероятность дорогостоящей кибератаки, и ряд громких нарушений привлек внимание заинтересованных сторон [2]. Услуги страхования становятся востребованы участниками информационных отношений. Риски информационной безопасности уже больше не являются проблемой только ИТ-подразделения. Так, в июле 2019 г. европейскими техническими комитетами ISO/IEC JTC 1/SC 27 выпускается в свет стандарт ISO/IEC 27102 «Information security management. Guidelines for cyber insurance». В декабре 2021-го Московским институтом электронной техники в инициативном порядке осуществляется перевод этого стандарта на русский язык и иницируется процедура принятия его как национального стандарта РФ. В 2021 г. приказом от 20 мая за номером 420-ст был утвержден национальный стандарт РФ ГОСТ Р 59516-2021 «Информационные технологии. Менеджмент информационной безопасности. Правила страхования рисков информационной безопасности».

Однако, плюс к предыдущему, результаты исследования современной обстановки в союзном государстве [3–6] позволяют утверждать, что страховая отрасль находится на пороге осознания актуальности страхового покрытия информационных рисков.

Тем не менее на текущий момент отношение к страхованию информационных рисков неоднозначное, в том числе законодателей РФ. Вопросы страхования рисков ИБ исключены из действующей доктрины ИБ 2016 г., национального проекта «Цифровая экономика» 2018 г.

Серьезным препятствием на пути к страхованию рисков ИБ, по мнению автора, является противоречивая ситуация, связанная с методическим обеспечением оценки рисков ИБ. Кратко ситуацию можно характеризовать так, что мы осознаем, что для внедрения страхования рисков ИБ, как экономического способа управления ИБ, требуется оценить риск ИБ. Однако на текущий момент, мы не знаем, как это сделать. Проблема в том, что на сегодня нет общепринятых методов и методик оценки риска ИБ объектов информатизации, подверженных угрозам ИБ. Так, исследования по разработке методического аппарата для организации и проведения аудита информационной безопасности, с целью оценить риск ИБ, проводятся в основном учеными инициативно. Судя по содержанию публикаций, стихийно создается некий математический задел, который в дальнейшем может быть использован для разработки методологии оценки риска ИБ.

1. О методологической проблеме

Для определения страховой премии требуется оценка устойчивости функционирования информационной инфраструктуры (ИИ) объекта информатизации, особенно для условий воздействия угроз информационной безопасности. Для чего необходимы исходные данные,

содержащие оценки устойчивости функционала отдельных элементов, входящих в состав соответствующей информационной инфраструктуры.

Если для штатных условий применения объекта информатизации имеется потенциальная возможность добыть репрезентативную статистику частных показателей устойчивости, что позволяет использовать ее для оценки количественные методы теории надежности. Зная оценки устойчивости отдельных элементов в штатных условиях применения, представляется возможным оценить, для этих же условий, функциональную устойчивость ИИ в целом. Некоторые из результатов фундаментальных исследований в области теории надежности сложных технических систем приведены в [7, 8].

Совсем другие условия для нештатного применения, репрезентативная статистика отсутствует в принципе, что порождает ряд особенностей при оценке функциональной устойчивости ИИ. Такая ситуация связана, прежде всего, с тем, что сами нештатные условия порождены воздействием угроз ИБ, связанных с поведением лиц, принимающих решения по ее обеспечению. Воздействия угроз в этом случае можно позиционировать как редкие явления, их длительность непредсказуема, сама обстановка при нештатных условиях весьма нестабильна. В этих условиях процессы исследуемых событий нельзя принять ни стационарными, ни эргодическими, ни стохастическими. Названные особенности не позволяют в полной мере применить классические методы математической статистики и теории вероятностей. Для решения задачи требуется разработка специальных методов оценки функциональной устойчивости с учетом вышеназванных особенностей. Такая неопределенность позиционируется как эпистатическая и зависит от уровня знаний об изучаемом объекте. Именно разделение риска ИБ со страховщиком является привлекательным в условиях воздействия угроз информационной безопасности. Однако адекватных инструментов оценки рисков ИБ для этих условий нет.

2. Содержательная постановка задачи оценки функциональной устойчивости

Пусть задана некая ИИ автоматизированной системы управления (АСУ), содержащая семейство взаимоувязанных элементов. Информационная инфраструктура, в состав которой входят эти элементы, подвергается активному воздействию угроз ИБ. На этапе проектирования ИИ для каждого из элементов были реализованы специальные меры, обеспечивающие некую их защищенность от угроз ИБ. Более того, в ставе ИИ имеется система восстановления ее функционала, обладающая неким производственным потенциалом (ресурсом) для восстановления функционала. Система восстановления реагирует на поражение ИИ восстановлением пораженных элементов, в результате чего восстанавливается функционал ИИ в целом. При этом расходуется соответствующий ресурс. Пусть требуется оценить функциональную устойчивость отдельных элементов ИИ.

Допущение. Для решения задачи принято допущение, суть которого заключается в том, что функция устойчивости элемента на заданном интервале времени $(0, T]$ реализации угрозы ИБ, представляется в виде композиции двух независимых функционалов. Эта композиция имеет вид

$$v(t, u, \Delta T, \lambda, \mu, \mathbf{P}) = K_{\text{ог}}(t, u, \Delta T) \varphi(t, \lambda, \mu, \mathbf{P}), \quad (1)$$

где $v(t, u, \Delta T, \lambda, \mu, \mathbf{P})$ – функция устойчивости элемента;

t – временной параметр оценки функции устойчивости;

u – показатель безотказности и восстанавливаемости элемента в штатных условиях применения, $u = \{T_n, T_b\}$, где T_n – средняя наработка на отказ элемента в штатных условиях;

T_b – среднее время восстановления работоспособности элемента. Значения частных показателей возможно получить на основе обработки соответствующих статистических данных, полученных в штатных условиях применения или из эксплуатационной документации;

ΔT – период времени от начала до окончания воздействия совокупности угроз ИБ;

$\lambda = \{F, n, T\}$ – характеристика угрозы ИБ, где F – совокупность функций распределения случайных интервалов времени η_i до очередной i -й угрозы ИБ, $F = \{F_i(t)\}$, где $F_i(t)$ – функция распределения случайного η_i интервала времени до i -й угрозы ИБ, $i = 1, 2, \dots, n$, n – количество воздействий угроз ИБ, T – момент времени окончания воздействий угроз информационной безопасности;

μ – частный показатель живучести элемента, характеризующий его способность восстанавливать, нарушенный в результате успешных воздействий угроз ИБ, функционал, $\mu = \{T_b, G\}$, где $T_b = \{\tau_{bi}^n, \tau_{bi}^b\}$ – совокупность нижнего и верхнего интервалов времени восстановления функционала; G – совокупность функций распределения случайных интервалов времени восстановления функционала элемента после воздействия i -й угрозы, $G = \{G_i(t)\}$, $i = 1, \dots, n$, n – число воздействий угроз ИБ, τ_{bi}^n – оценка нижнего интервала восстановления функционала после воздействия i -й угрозы, τ_{bi}^b – оценка верхнего интервала восстановления функционала после воздействия i -й угрозы ИБ.

Оценка параметров $\{\tau_{bi}^n, \tau_{bi}^b\}$ осуществляется либо с помощью экспертных методов, либо в результате соответствующих учений, деловых игр или специальных исследований;

P – совокупность частных показателей живучести элемента, характеризующая его защищенность, т.е. способность сохранять требуемый функционал в результате отражения совокупности угроз ИБ. В качестве такого показателя принята совокупность вероятностей поражения элемента при отражении угрозы ИБ, $P = \{p_i\}$, где p_i – вероятность поражения элемента при воздействии i -й угрозы ИБ, $i = 1, \dots, n$, n – число воздействий угроз ИБ. Оценка вероятностей p_i осуществляется либо с помощью экспертных методов, либо добывается в результате соответствующих учений, деловых игр или статистического моделирования. Если при моделировании требуется оценка живучести с неким запасом, то можно рекомендовать $p_i = 1$. В этом случае принимается, что живучесть обеспечивается за счет способности оперативно восстанавливать функционал. Если оценка осуществляется в полной неопределенности, то $p_i = 0,5$;

$K_{ог}(u, t) = K_{г}(u) P(t, \Delta T)$ – нестационарный коэффициент оперативной готовности элемента, определяемый вероятностью его безотказной работы в течение времени реализации угрозы ИБ и устранения ее последствий, $\Delta T = (0, T]$, где $K_{г}(u)$ – коэффициент готовности элемента, рассчитанный для штатных условий его применения, $P(t, \Delta T)$ – вероятность безотказной работы элемента в течение периода времени ΔT ;

$\varphi(t, \lambda, \mu, P)$ – функция живучести элемента в условиях угрозы ИБ.

Для большинства практических случаев значение $K_{ог}(u)$ на периоде времени ΔT очень близко к единице, а значение функции живучести на этом же периоде неизмеримо меньше $\varphi(t, \lambda, \mu, P) \ll K_{ог}(u)$. С учетом этого утверждения формулу (1) можно привести к виду

$$v(t, \lambda, \mu, u, P) \approx \varphi(t, \lambda, \mu, P),$$

т.е. функция устойчивости элемента, для условий воздействия угроз ИБ, может быть приближенно заменена функцией живучести.

Ранее автором исследовалась возможность решения подобной задачи с помощью статистического моделирования методом Монте-Карло. Авторский подход к моделированию приведен в [9, 10]. При этом исходные данные для моделирования добывались экспертными методами.

Заключение

Существенным препятствием внедрения страхования информационных рисков в управление информационной безопасности является отсутствие адекватного и общепринятого методического обеспечения оценки рисков ИБ. Требуется усилия по разработке специальных методов, позволяющих оценить риски применительно к страхуемым объектам информатизации находящихся под целенаправленными угрозами ИБ.

Литература

1. Businesswire: Global Cyber Insurance Market Report 2019–2025 (Dec. 2019). www.businesswire.com/news/home/20191213005215/en/Global-Cyber-Insurance-MarketReport-2019-2025-Market.
2. Attacks on Russian companies in the 3rd quarter of 2022. Rostelecom-Solar Report, Moscow 2022: <https://ict.moscow/research/ataki-na-rossiiskie-kompanii-v-iii-kvartale-2022-goda/?amp&> (дата обращения: 01.03.2023).
3. Рубан, Т.Е. Страхование информационных рисков и его развитие в Республике Беларусь / Т.Е. Рубан, А.В. Рожко // Проблемы развития национальной экономики на современном этапе: Материалы Международной научно-практической конференции, Тамбов, 25 ноября 2019 года / Ответственный редактор А.А. Бурмистрова [и др.]. – Тамбов: Издательский дом «Державинский», 2019. – С. 154–159.
4. Свириденкова, М.А. Страхование информационных рисков как современный инструмент управления информационной безопасностью / М.А. Свириденкова // Экономика и предпринимательство. – 2021. – № 2(127). – С. 1328–1331. – DOI 10.34925/EIP.2021.127.2.267.
5. Концепция информационной безопасности Республики Беларусь: в ред. пост. Совета Безопасности Республики Беларусь от 18.03.2019 г. № 1 / Нац. центр правовой информации Республики Беларусь. – Минск, 2019. (ст. 68)
6. Зайцева, М.А. Страхование киберрисков и его развитие в Республике Беларусь / М.А. Зайцева, Н.С. Ананенко // Интеграция и развитие научно-технического и образовательного сотрудничества – взгляд в будущее: Сборник статей II Международной научно-технической конференции. В 3 томах, Минск, 11–12 декабря 2019 года. Том 3. – Минск: Белорусский государственный технологический университет, 2020. – С. 35–38.
7. Надежность и эффективность в технике. Справочник Том № 5. Проектный анализ надежности / под ред. В.И. Патрушева и А.И. Рембезы. – М.: Машиностроение, 1989. – 376 с.
8. Гнеденко Б.В., Беляев Ю.К., Соловьев А.Д. Математические методы в теории надежности. – М.: Наука, 1965. – 524 с.
9. Voevodin V.A., Burenok D.S. and Cherniaev V.S. «Technique for Detecting Computer Attacks on a Wi-Fi Networks» 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 2022, pp. 487–492, DOI 10.1109/ElConRus54750.2022.9755703.
10. Voevodin, V.A. Monte Carlo method for predicting the stability of the functioning of the informatization object in the conditions of massive computer attacks. International Conference «Marchuk Scientific Readings 2021» (MSR-2021) Journal of Physics: Conference Series 2099 (2021), DOI 10.1088/1742-6596/2099/1/012070.

ПРИОРИТИЗАЦИЯ СВЕДЕНИЙ ОБ УЯЗВИМОСТЯХ, АТАКАХ, ЭКСПЛОЙТАХ, ИСПОЛЬЗУЕМЫХ ДЛЯ ПРОГНОЗИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, НА ОСНОВЕ ПУБЛИКАЦИЙ В СЕТИ ИНТЕРНЕТ

М.А. ТАРЕЛКИН, А.А. ТЕПЛИНСКИХ

*Федеральное автономное учреждение «Государственный научно-исследовательский институт проблем технической защиты информации
Федеральной службы по техническому и экспортному контролю»,
г. Воронеж, 394020, Российская Федерация*

Введение

В настоящее время задача прогнозирования угроз безопасности информации (УБИ) является одной из наиболее актуальных в области защиты информации. Эффективное прогнозирование начинается с работы с входными данными для системы прогнозирования УБИ, получаемыми из различных источников, таких как:

- базы данных уязвимостей и эксплойтов (NVD, kb-CERT, CXSecurity, ExploitDB и т.д.);
- информационные ресурсы исследователей программного обеспечения (ПО) (SecureList, Talos blog, Zero Day Initiative и др.);
- новостные информационные ресурсы (SecurityLab, Anti-Malware, ZDnet, ThreatPost, CNews и проч.);
- социальные сети (телеграм, твиттер);
- уведомления разработчиков программного обеспечения (Microsoft, Oracle, Cisco, Red Hat Linux, Gentoo и т.п.);
- международные стандарты, содержащие сведения о способах реализации угроз, шаблоны атак и т.д. (CWE, CAPEC, ATT&CK и др.).

Получение данных из этих источников связано с необходимостью обработки больших объемов информации, при этом особую сложность вызывают масштабные массивы разнородных данных, получаемых с применением зачастую нескольких отличающихся технологий [1]. Все это обуславливает, во-первых, необходимость решения задачи приоритизации сведений, то есть выделения приоритетных из них, которые позволяют выявить наиболее важные для практики организации защиты уязвимости, разработанные или разрабатываемые для их эксплуатации эксплойты и, конечно, угрозы безопасности информации, которые могут быть реализованы в прогнозируемый период времени. Во-вторых, весьма востребованным становится автоматизация процессов поиска, обработки и приоритизации указанных сведений. В данном докладе излагается один из подходов к решению указанной задачи.

1. Краткая характеристика источников информации об угрозах безопасности информации

Основные источники сведений об УБИ разделяют на структурированные и неструктурированные, что обусловлено способами представления информации. В структурированных источниках, например, таких, как базы данных уязвимостей и эксплойтов сведения представляются в строго формализованном виде. Каждая запись содержит строго формализованные поля (такие как, «Описание уязвимости», «Вектор опасности», «Ссылки на источники»). Для структурированных источников характерен значительный объем ежедневных публикаций, например, для NVD – порядка 80 публикаций в день. Одновременно стоит отметить, что получение информации из большинства структурированных источников упрощается наличием прикладных программных интерфейсов (API) и возможностями получения выгрузок сведений в XML, JSON и т.п. форматах.

Особенностью неструктурированных источников является представление информации в произвольном виде. Для формата новостной статьи или блога исследователя может иметь место представление сведений, например, об идентификаторе уязвимости в виде ссылки, картинки или текстового значения, что создает определенные трудности при обработке таких разноформатных сведений. Существуют RSS-каналы, позволяющие упростить сбор из некоторых неструктурированных (в основном новостных) источников, но сведения, содержащиеся в таких публикациях, остаются разнородными, а форматы их представлений трудно формализуемыми.

2. Основные особенности и сложности, связанные со сбором исходных данных для прогнозирования УБИ

Исходя из приведенных кратких характеристик источников сведений об УБИ, обозначим ключевые особенности и основные сложности, связанные со сбором исходных данных для их прогнозирования (рис. 1).

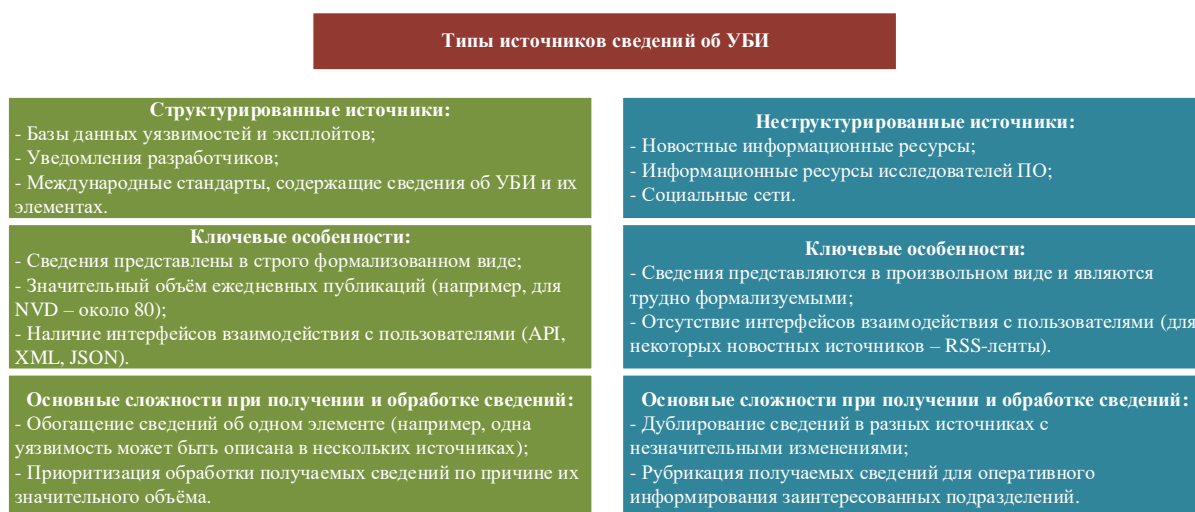


Рисунок 1. – Ключевые особенности и сложности, связанные со сбором исходных данных для прогнозирования УБИ

С учетом указанных особенностей были сформулированы ключевые требования к системе мониторинга, сбора и обработки данных (система МСОД), основными из которых являлись:

- возможность оперативного сбора сведений из структурированных и неструктурированных источников;
- извлечение и обобщение необходимых структур данных из различных источников;
- дедубликация аналогичных публикаций для сокращения времени обработки и снижения размерности обрабатываемых данных.

Требования были реализованы путем внедрения:

- одновременной возможности применения инструмента WebScrapер и имплементации разработанных на языке Python программ для сбора данных (парсеров);
- механизма концептов (структурных элементов, позволяющих автоматически выделять и обобщать необходимые сведения, содержащиеся в анализируемой публикации).

3. Приоритизация сведений об уязвимостях, получаемых из структурированных источников

Огромное количество публикаций из структурированных источников в сети Интернет, которые приходится просматривать в ходе сбора необходимых сведений, обусловило необходимость выделения из них важных сведений и исключения из дальнейшего анализа тех, которые не представляют интереса для ведения банка данных угроз ФСТЭК России, то есть расставления приоритетов или приоритизации сведений.

Далее такая приоритизация рассматривается на примере обработки сведений об уязвимостях ПО. Для обоснованного присвоения приоритета уязвимостям был выбран механизм тегирования, в котором использовались соответствующие количественные показатели, что позволяет формализовать процедуру приоритизации. В частности, в интересах приоритизации сведений об уязвимостях использовались:

интегральный показатель S , зависящий от частных показателей – прямых (наличие эксплойта, приоритетность ПО, уровень критичности уязвимости, наличия сведений об использовании уязвимости в атаках);

косвенных показателей, таких как наличие публикаций сведений об уязвимостях в новостных источниках и присутствие их в рассылке НКЦКИ.

В ходе исследований было установлено, что целесообразно применение следующих тегов для приоритизации уязвимостей (по результатам опроса 10 экспертов):

#НКЦКИ – уязвимости, полученные от НКЦКИ;

#Новости – уязвимость является широко обсуждаемой в СМИ и социальных сетях (telegram, twitter, youtube, хакер, securitylab, ZDI и др.);

#Эксплойт – эксплуатируемые уязвимости, о которых имеются сведения о рабочем эксплойте (Paket Storm, Exploit-DB и др.);

#Критические – оценка CVSS v3 в интервале от 9 до 10;

#Приоритетное ПО – программное обеспечение, широко распространенное в ГИС, КИИ;

#Атака – имеет место информация об использовании уязвимости при проведении компьютерных атак (CISA, выгрузка из Metasploit и др.).

Присвоение уязвимости определенного тега влияет на ее приоритетность. Значение поля приоритета обозначим S (диапазон значений от 0 до 1000).

В результате экспертного анализа сведений об уязвимостях определены следующие показатели, которые могут быть использованы для оценки приоритетности уязвимостей.

Показатель «НКЦКИ» характеризует наличие сведений об уязвимости в бюллетенях, рассылаемых НКЦКИ.

Показатель «Новости» характеризует количество релевантных (достоверных) источников (ресурсов в сети Интернет), в которых упоминается уязвимость.

Показатель «Эксплойт» характеризует наличие или отсутствие сведений о средстве для эксплуатации уязвимости.

Показатель «Критические» характеризует уровень опасности уязвимости в соответствии с метриками CVSS v3.

Показатель «Приоритетное ПО» характеризует широко распространенное ПО, применяемое в ГИС и КИИ.

Показатель «Атака» характеризует наличие у эксперта сведений об использовании уязвимости при проведении компьютерных атак.

Итоговая оценка вычисляется по следующей формуле:

$$S = v \cdot \sum_{i=1}^I w_i \cdot p_i + z \cdot \sum_{j=1}^J q_j \cdot p_j, \quad (1)$$

где p_i – числовое значение прямого показателя оценки уязвимостей, $i = \overline{1, I}$;

p_j – числовое значение косвенного показателя оценки уязвимостей, $j = \overline{1, J}$;

I, J – количество прямых и косвенных показателей соответственно;

w_i, q_j – весовые коэффициенты прямых и косвенных показателей соответственно,

$$\sum_{i=1}^I w_i = 10, \quad \sum_{j=1}^J q_j = 10;$$

v, z – весовые коэффициенты группы прямых и косвенных показателей оценки уязвимостей, $v + z = 10$.

В таблице 1 приведены оценки значений базового набора показателей и соответствующие им весовые коэффициенты, заданные экспертным методом на основе опыта ведения БДУ ФСТЭК России [2].

Таблица 1. – Оценки значений базового набора показателей

№ (i, j)	Показатель	Вес (w_i, q_j)	Значение	Оценка (p_i, p_j)
Прямые показатели ($v = 7$)				
1	Эксплойт	3	Да	10
			Нет (или нет данных)	0
2	Приоритетное ПО	3	Да	10
			Нет	0
3	Критическая	2	Да	10
			Нет	0
4	Атака	2	Да	10
			Нет (или нет данных)	0
Косвенные показатели ($z = 3$)				
1	Новости	2	Больше или равно 10	10
			От 5 до 9	5
			Менее 5	0
2	НКЦКИ	8	Да	10
			Нет (или нет данных)	0

Уровень приоритетности уязвимостей принимает значения в соответствии с таблицей 2.

Таблица 2. – Уровни приоритетности уязвимостей

Уровень приоритетности	Итоговая оценка по интегральному показателю (S)
Критический	≥ 900
Высокий	от 600 до 899
Средний	от 400 до 599
Низкий	< 399

4. Рубрикация получаемых сведений для оперативного информирования заинтересованных подразделений

Автоматическая рубрикация сведений проводится путем поиска в информационном сообщении ключевых слов из заранее сформированного перечня.

В результате автоматической рубрикации могут возникать ошибки первого и второго рода, поэтому результаты автоматической рубрикации должны быть проверены оператором, осуществляющим управление процессом сбора.

Для оценки качества результатов рубрикации наиболее распространенной практикой является использование следующих показателей [3]: точность; полнота; интегральная метрика (например, F-мера).

Точность системы в пределах класса – доля публикаций, которые были верно классифицированы, относительно всех публикаций, отнесенных системой к рассматриваемому классу.

$$P = \frac{TP}{TP + FP}, \quad (2)$$

где TP – истинно-положительные решения об отнесении к классу;

FP – ложно-положительные решения об отнесении к классу.

Полнота системы – доля публикаций рассматриваемого класса, найденных классификатором, относительно всех публикаций этого класса в тестовой выборке:

$$R = \frac{TP}{TP + FN}, \quad (3)$$

где TP – количество истинных решений об отнесения к классу;

FN – количество ложных решений об отнесении к классу.

В качестве интегрального показателя, характеризующего как точность, так и полноту классификации публикаций, наиболее часто рассматривают F-меру, представляющую собой гармоническое среднее между точностью и полнотой.

$$F = (\beta^2 + 1) \cdot \frac{P \cdot R}{\beta^2 \cdot P + R}, \quad (4)$$

где β – коэффициент, регулирующий влияние на результирующее значение точности или полноты ($0 < \beta < 1$, если точность более важна, чем полнота;

$\beta > 1$ – полнота более важна, чем точность, $\beta = 1$ – точность и полнота равнозначны).

Для данной задачи классификации приемлемым считается значение F-меры большее или равное 0,7 (более двух третей публикаций будут отнесены в нужную группу).

Указанный показатель был достигнут путем корректировки множества ключевых слов и задания их комбинаций при помощи регулярных выражений.

Следует подчеркнуть, что уязвимости являются структурными элементами описания угроз, поэтому тенденции, связанные с публикацией сведений об уязвимостях за определенные временные интервалы, позволяют сделать прогноз об атаках на информационные системы, в которых распространены определенные программные продукты или применяются те или иные технологии.

Заключение

Сведения об УБИ включают множество разнородных элементов, которые необходимы для всестороннего их описания. Полное структурированное описание элементов УБИ позволяет перейти к процессам прогнозирования. Предложенный подход, позволяющий создавать произвольные концепты (как составляющие описания УБИ), в перспективе дает возможность находить в ходе обработки сведений неявные связи между ними и скрытые закономерности и, как следствие, повысить эффективность процесса прогнозирования УБИ.

Литература

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

3. Оценка классификатора (точность, полнота, F-мера) [Электронный ресурс] – Режим доступа: <http://bazhenov.me/blog/2012/07/21/classification-performance-evaluation.html>.

Авторы

Тарелкин Михаил Андреевич, старший научный сотрудник ФАУ «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю», г. Воронеж, Россия. Email: gniii@fstec.ru

Теплинских Александр Андреевич, научный сотрудник ФАУ «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю», г. Воронеж, Россия. Email: gniii@fstec.ru

ПОСТРОЕНИЕ ОТРАСЛЕВЫХ И КОРПОРАТИВНЫХ ЦЕНТРОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

М. КРАСНИЦКИЙ

*Технологическая компания в сфере информационной безопасности
ООО «МультиТек Инжиниринг» г. Минск, Республика Беларусь*

Введение

Для обеспечения киберустойчивости предприятий и организаций необходимо:

- 1) получать достоверную информацию о событиях ИБ и оперативной обстановке;
- 2) обеспечить четкую и скоординированную работу ИБ-, ИТ-специалистов, других служб в процессах предотвращения, детектирования, анализа инцидентов ИБ и реагирования на них.

Для решения этих задач компания ООО «МультиТек Инжиниринг» в течение 4 лет разрабатывала, проверяла на практике и совершенствовала концепцию создания корпоративных центров управления информационной безопасностью (ЦУИБ).

1. Подход

Сосредоточив наиболее дорогостоящие и высокотехнологичные средства защиты и высококвалифицированные кадры по ИБ в едином центре, обеспечив интеграцию средств защиты информации, установленных в филиалах территориально-распределенного предприятия, с центром, предприятие получит возможность контролировать и своевременно реагировать на угрозы, возникающие в информационной системе (ИС).

За счет такой централизации всегда можно оценить состояние ИБ в целом по предприятию, с опережением внедрять меры предупреждения выявленных инцидентов для ИС филиалов, управлять системой защиты информации ИС предприятия.

2. Структура ЦУИБ

ЦУИБ базируется на трех составляющих: люди (команда специалистов), процессы ИБ, технологии.

3. Формирование команды, разработка и внедрение процессов

В ЦУИБ выделяются 3 основные роли: руководитель, аналитик и оператор.

4. Выбор и внедрение технологий ЦУИБ

Эффективность функционирования ЦУИБ в значительной степени зависит от корректного выбора, внедрения, эксплуатации и сопровождения технологий защиты информации.

Заключение

Подходы, рассмотренные в докладе, могут быть использованы предприятиями и организациями при создании отраслевых и корпоративных центров кибербезопасности, предусмотренных Указом Президента Республики Беларусь № 40 от 14.02.2023 г. «О кибербезопасности».

МЕХАНИЗМЫ МОБИЛИЗАЦИИ БОЛЬШИХ СОЦИАЛЬНЫХ ГРУПП ПРИ ПРОВЕДЕНИИ ПСИХОЛОГИЧЕСКИХ ОПЕРАЦИЙ В ЗОНЕ ИНТЕРЕСОВ

Е.А. РАФАЛЬСКАЯ

*Учреждение образования «Международный государственный экологический институт имени А.Д. Сахарова» Белорусского государственного университета,
г. Минск, Республика Беларусь*

С.П. ЛАРИН

Государственное учреждение «Научно-исследовательский институт Вооруженных Сил Республики Беларусь», г. Минск, Республика Беларусь

Глобализация мира, продолжающаяся борьба ведущих стран мира за сферы влияния и стратегические источники ресурсов свидетельствуют об угрозе разжигания конфликта в любой точке планеты. При этом вооруженная борьба не всегда является главной и определяющей, происходит смещение акцента в сторону не силовых методов решения поставленных задач. Инспирирование современного конфликта в большей степени представляет собой противостояние в сфере общественного сознания, где ведется борьба взглядов, принципов, морального духа. В этом плане ведущую роль играют информационные операции (ИО). При грамотном планировании и реализации мероприятий в информационной сфере обеспечивается возможность гибкой и быстрой доставки требуемой информации, адаптированной для восприятия целевой аудитории противостоящей стороны, формируя благоприятные условия для достижения военных, политических, экономических целей.

Не случайно особое внимание США и европейскими странами уделяется развитию теории применения вооруженных сил с опорой на максимальное использование информационных технологий и информационных ресурсов государства. Отдельные положения указанной теории уже реализованы в руководящих документах. Создаются соответствующие управленческие структуры, осуществляется целенаправленная подготовка специалистов, получают развитие технологии, способы и формы ведения информационных операций.

Самым благоприятным объектом психологического воздействия при проведении ИО является гражданское население, как наиболее уязвимое с точки зрения критического восприятия информации. В связи с этим значительное внимание уделяется развитию технологий, позволяющих мобилизовать большие социальные группы для формирования протестного потенциала на определенной территории, входящей в зону интересов.

В настоящее время американские ученые мобилизационные технологии определяют, как «коллективную активизацию населения посредством интернет-ресурсов для участия в акциях протеста» [2]. Они обладают присущими социальным медиа характеристикам: оперативностью, доступностью и интерактивностью (как пример – события «арабской весны»). В отечественной научной литературе не выработан единый подход к пониманию термина «мобилизационные технологии», однако частично сущность данного понятия определена в толковом словаре С.И. Ожегова и Н.Ю. Шведовой: «мобилизация – ...приведение кого-нибудь или чего-нибудь в состояние, обеспечивающее успешное выполнение какой-нибудь задачи» [3].

Изучением особенностей коллективного поведения населения, участвовавших в акциях протеста, начали заниматься еще в начале 20-го века ученые США, такие как Доусон, Геттис, Г. Блюмер и Н.Дж. Смелзер. Они пришли к выводу, что для понимания и описания данного явления, в том числе в интересах прогнозирования с возможностью контроля массовых волнений, необходимо проводить анализ причинно-следственных механизмов каждого из этапов массовой мобилизации. Это объясняется тем, что некоторые факторы и механизмы, которые являются ключевыми на одном этапе, практически не имеют причинно-следственной значимости на других этапах, а ряд факторов могут резко измениться в содержании и значении

(с усиливающих к ослабляющим). По их мнению, такой теоретический подход облегчает интеграцию большого и разнообразного свода научных исследований в структурированный анализ массовой мобилизации, который позволяет детально провести исследование и сравнить этапы различных массовых протестов.

Американские ученые выделяли четыре этапа массовой мобилизации, названия которых представлены в таблице 1.

Таблица 1. – Этапы массовой мобилизации

Исследования	Этапы массовой мобилизации
Доусон, Геттис Модель последовательности мобилизации, 1929 г.	– предварительная стадия социальных волнений; – стадия коллективного возбуждения; – стадию формальной организации; – институционализация
Гёрберт Блүмер 1951 г.	– социальное брожение; – популярность; – формализация; – институционализация
Нил Джозеф Смэлзер Теория коллективного поведения, 1962 г.	– напряжение; – обвинение; – предложение решения; – устранение причины напряжения

Каждый этап – это период в жизненном пути массовой мобилизации, отличающийся уникальными особенностями. Он может состоять из нескольких дней, месяцев или (реже) лет. Каждый этап обладает уникальными факторами и механизмами, которые являясь ключевыми на одном этапе, на других – не имеют причинно-следственной связей. Поэтому они должны изучаться как отдельно каждый, так и во взаимосвязи друг с другом.

Более поздние исследования выделяют **три основных этапа массовой мобилизации: зарождение, протест и результат.**

Этап зарождения (исток) массовой мобилизации – это стадия, на которой значительное количество людей становится недовольными (обиженными) и мотивированными к протесту. Как правило, включает следующие компоненты: недовольство (обида) и мотивация протеста.

В ходе данного этапа осуществляется подготовка «неактивистов» к действиям и сами протесты. Специалисты отмечают, что даже принятие органами государственного управления непопулярных социально-политических решений могут не быть причинами для активного выражения недовольства большими социальными группами в связи с психологическими особенностями населения и свойственными ему типовыми реакциями. Исследователи сходятся во мнении о роли когнитивной и эмоциональной составляющей при мобилизации населения к участию в протестах, хотя в вопросах объяснения недовольства и формирования мотивация такого единодушия нет.

Типы протеста часто зависят от причинных механизмов на стадии возникновения:

в одних случаях необходимо сначала достичь консенсуса по определенному вопросу, прежде чем появится какой-либо потенциал для мобилизации [4].

в других – консенсус существует, но нет достаточной мотивации или слишком большой страх, чтобы что-то с этим сделать, как в случае гражданских разочарований.

Таким образом, возникновение недовольства и мотивации к протесту – это два необходимых, но различных аспекта мобилизации.

Этап протеста характеризуется волной протестных акций большого количества людей (тысяча или более), которые либо физически мобилизуются в одном месте (протест, марши, флеш-мобы), либо координируют свои действия в заданные сроки (бойкот, забастовка).

В данном этапе выделяют четыре основных компонента:

формы политического давления;
степень организованности мобилизации;
психологические процессы, лежащие в основе массовой мобилизации;
типы внешних сил, влияющих на массовую мобилизацию.

Анализ этих компонентов дает ответ о влиянии внутренних и внешних факторов в ходе этапа.

Этап результат. Каждая попытка массовой мобилизации имеет результат, начиная от полного успеха, такого как смена власти или принятие законов, до полного провала – полное отсутствие социальных и политических изменений, или даже непреднамеренных негативных последствий, включая репрессии и противодействие протестным движениям. Соответствующий результат может иметь ближайшую (краткосрочную) или долгосрочную цели.

Так, ближайшая цель является достигнутой, когда массовая мобилизация приносит немедленные ощутимые уступки или явные победы в разгар протестов, таких как отставка президента (например, Бен-Али в Тунисе и Мубарака в Египте) или общественно-политическое принятие требований протестующих.

В случае если результат получен в течение непродолжительного периода времени, т.е. после того, как протесты были отклонены или исчезли, характер цели также определяется как краткосрочный. (Например, принятие Закона о гражданских правах и Закона об избирательных правах в Соединенных Штатах через несколько месяцев после окончания массовых протестов в Бирмингеме и Сельма-Монтгомери.)

Мобилизация также может привести и к долгосрочным результатам, которые можно оценить только в исторической перспективе, таким как изменения в поведении, культуре или идентичности, серии политических решений или запуск социально-политических процессов с неясными конечными целями [5, 6].

В заключение необходимо отметить, что национальная безопасность страны – это состояние защищенности государств от внутренних и внешних угроз, которые могут иметь скрытый и явный характер. Поэтому важно для органов государственного управления проводить анализ процессов мобилизации (в том числе скрытых) больших социальных групп для своевременного вскрытия угроз национальной безопасности и проведения соответствующих мероприятий по противодействию и нейтрализации дестабилизации внутривнутриполитической обстановки.

Литература

1. Strategic information warfare rising [Electronic resource] / R.C. Molander [et al.] // RAND's National Defense Research Institute. – Mode of access: http://www.rand.org/pubs/monograph_reports/MR964/. – Date of access: 04.07.2019.

2. Ильичева, Ю.А. Мобилизационные технологии: сущность, предпосылки возникновения, основные инструменты и средства/ Ю.А. Ильичева // Электронный научный журнал «Медиаскоп», вып. № 2, 2013 Адрес доступа: <http://www.mediascope.ru>. – Дата доступа: 15.11.2020.

3. Ожегов, С.И. Толковый словарь русского языка. 100 000 слов, терминов и выражений. / С.И. Ожегов, Н.Ю. Шведова // 4-е изд., доп – М.: Изд: «А ТЕМП». – 944 с.

4. Klandermans, B. Collective political action. In Oxford handbook of political psychology. – Oxford: Oxford University Press, 2003.

5. Foran, J. Discourses and social forces: The role of culture and cultural studies in understanding revolutions. In Theorizing revolutions. – New York: Routledge, 1997.

6. Isaac, L. Movement of movements: Culture moves in the long civil rights struggle. Social Forces, 87, 2008. – P. 33–63.

ИНФОРМАЦИОННАЯ И КИБЕРБЕЗОПАСНОСТЬ ИНФРАСТРУКТУР СОЮЗНОГО ГОСУДАРСТВА КАК КЛЮЧЕВОЙ ФАКТОР ОБЕСПЕЧЕНИЯ РЕГИОНАЛЬНОЙ БЕЗОПАСНОСТИ

А.В. ФЕДОРЦОВ

*Государственное учреждение «Научно-исследовательский институт
Вооруженных Сил Республики Беларусь», г. Минск, Республика Беларусь*

Введение

Каждое из государств Союза Беларуси и России к настоящему времени уже создало необходимую национальную нормативно-правовую базу в области обеспечения безопасности собственного информационного и киберпространства. Нормативно-правовая база в данном контексте включает как национальное законодательство, так и международные конвенции (документы), которые были подписаны и приравнены к законам. В свою очередь, во взаимосвязи с содержанием имеющейся базы представленными государствами были определены соответствующие национальные концепции, стратегии и доктрины [1, 2].

В силу того, что информационному и киберпространству, как правило, свойственна глобальность и трансграничность, вызовы и угрозы национальной безопасности, проявленные в выделенных сферах относительно одного государства, входящего в состав Союза, имеют не только национальное проецирование, но и обозначают вызовы и угрозы различным объединениям обоих государств, то есть региональной безопасности. К тому же эти вызовы и угрозы государству из обозначенного числа зачастую реализуются комплексно, а самостоятельное решение возникающих при этом проблем национальной безопасности прежними методами и без поддержки извне становится затруднительным.

Из вышесказанного следует, что целое (безопасность информационного и киберпространства государств – членов Союза) обладает свойствами, которыми не обладают составляющие его части (безопасность этих сфер отдельно взятых государств). Именно такой предметный анализ складывающихся условий указывает на необходимость независимого обеспечения информационной и кибербезопасности инфраструктур Союзного государства в контексте региональной безопасности.

Технологические аспекты обеспечения информационной и кибербезопасности инфраструктур. Термин «*инфраструктура*» изначально появился в 20-е гг. XX в. в военной сфере и означал комплекс сооружений, объектов, обеспечивающих действия вооруженных сил. С течением времени теоретиками понятие «*инфраструктура*» было приведено к общему виду и трактовалось как «совокупность элементов, обеспечивающих бесперебойное функционирование взаимосвязей объектов и субъектов любой системы».

Были выделены следующие основные функции инфраструктуры:

активная (регулирующая) – упорядочение взаимодействия элементов посредством воздействия на взаимосвязи, изменяя и упорядочивая их по определенному принципу, определяемому информацией;

пассивная (техническая) – обеспечение функционирования взаимосвязей между элементами системы.

Относительно информационной инфраструктуры государства можно отметить, что, например, согласно Концепции [1] это «совокупность технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации».

В соответствии с Указом [3] к критически важной информационной инфраструктуре (КВИИ) Беларуси относят объекты организаций:

- электросвязи;
- обмена трафиком;
- телекоммуникационных услуг;
- информационно-вычислительных услуг;

- банковских услуг;
- электронных услуг;
- электроэнергетики;
- производства удобрений и нефтепереработки;
- переработки целлюлозы;
- газотранспортных и нефтетранспортных услуг;
- страхования.

В России к КВИИ относят объекты следующих организаций [4]:

- связи;
- банковской сферы;
- энергетики;
- транспорта;
- горнодобывающей, металлургической и химической промышленности;
- науки;
- здравоохранения.

Указанные выше перечни КВИИ, безусловно, могут со временем уточняться. Однако обеспечение их информационной и кибербезопасности будет оставаться приоритетным в контексте региональной безопасности.

Дефиниция «*информационная безопасность*» (в самом узком варианте – «*защита данных*») как в Беларуси, так и в России подразумевает комплекс мер, направленных преимущественно на сохранение основных свойств информации – конфиденциальности, целостности и доступности (КЦД).

В соответствии с теорией систем, основополагающим фактором информационной безопасности (ИБ) является именно угроза в информационном пространстве. Отсутствие угрозы конкретному информационному активу обуславливает отсутствие предмета обсуждения.

В зависимости от этапов жизненного цикла технического средства рассматривают кортеж базовых факторов: дефект безопасности (*weakness*), уязвимость (*vulnerability*), угроза, риск. Именно адекватность и полнота систематизации/описаний указанных факторов обуславливают уместность, результативность и эффективность методов обеспечения ИБ.

Понятие «*кибербезопасность*» (КБ), в отличие от ИБ, имеет зарубежное происхождение и носит нестрогий характер по причине отождествления со сферой военных операций в киберпространстве (КП) как новом театре военных действий. Отдельные стандарты зарубежных государств указанное понятие представляют условно двумя трактовками:

- как выраженная активная составляющая (*offensive security*) ИБ, а именно – сохранение свойства защищенности цифровых активов от кибернетических (обычно целенаправленных) атак, по-другому от *APT (Advanced Persistent Threat)*;

- как синоним ИБ в некотором сегменте КП (фактически это сленг ИБ), то есть – как сохранение свойства защищенности сегмента цифровых активов (данных в электронном виде или абстрактных виртуальных приложений) от соответствующих киберугроз в традиционной парадигме КЦД.

Так, в глоссариях Комитета по системам национальной безопасности США (CNSSI) и Национального института стандартов и технологий США (NIST), а также в ряде американских нормативно-методических фреймворках приводится «пронаступательный» вариант дефиниции КБ [5]. Ряд специальных публикаций NIST вообще тривиально КБ сводит к «предотвращению, обнаружению и реагированию на атаки» [6]. Разумеется, аналогичной позиции придерживаются практикующие ученые по кибербезопасности НАТО [7]. Вариант «сленговый» тоже весьма распространен, его модификации приводятся в американских политических документах, словарях [8].

Можно резюмировать, что эффективность методов КБ напрямую зависит от описания кибернетических атак. Виды, категории, этапы («*техники*»), методики («*тактики*») и средства проведения кибератак составляют суть тематики КБ. Соответственно, отмечаются именно две отличительные черты понятия КБ:

- наличие угрозы реализации кибернетической атаки (как наступательной сетевой составляющей обеспечения ИБ);
- цифровые активы, подлежащие компрометации.

Исходя из изложенного, имеет место выраженная бифуркация свойства безопасности информационной инфраструктуры государства (рис. 1).

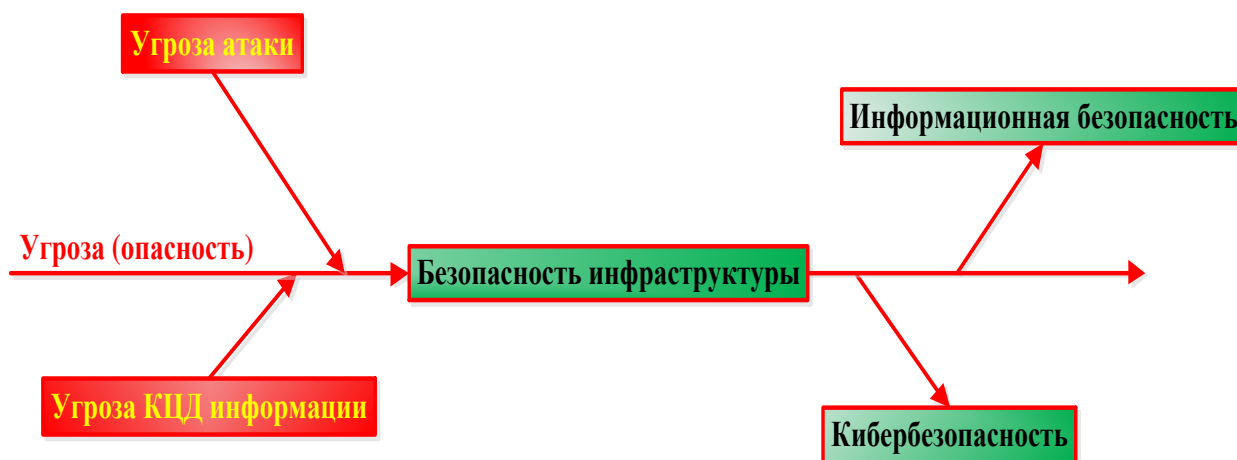


Рисунок 1. – Бифуркация свойства безопасности информационной инфраструктуры

Вместе с тем, совершенно очевидно, что мировое сообщество рассматривает КБ как элемент обеспечения ИБ в целом. Так как методы ИБ и КБ имеют когерентные прикладные цели, задачи и реализации, то есть лежат, главным образом, в плоскости технических наук, но, разумеется, – как любая сложная проблематика – на стыках и пересечениях, например, военных, политических, социальных, юридических и др.

Во всех трех системах международной стандартизации ISO, IEC и ITU также упоминается термин КБ. Стандарт ISO/IEC 27100: 2020 дает определение КБ как сохранение свойства защищенности активов (общества, организации, человека) от киберрисков, связанных с эксплуатацией уязвимостей в КП – цифровой среде в самом широком смысле. Аналогичную интерпретацию дает технический стандарт ITU X.1205: 2008 – те же угрозы и риски КИД в ограниченной (сетевой) среде. Упоминание рисков, по мнению авторов технических нормативных актов, подчеркивает проактивную деятельность по управлению КБ. В свою очередь, стандарт ISO/IEC 27032: 2012 определяет связи понятия «кибербезопасность» с безопасностью приложений, безопасностью сетей, безопасностью Интернета и, соответственно, защитой КВИИ в КП, как показано на рисунке 2.



Рисунок 2. – Терминологический базис понятия «*кибербезопасность*» согласно стандарту ISO/IEC 27032: 2012

Согласно тому же стандарту «*киберпространство*» определяется как «комплекс среды и, как следствие, в результате взаимодействия людей, программного обеспечения и услуг в Интернете с помощью технологии устройств и сетей, подключенных к ней, которых не существует в любой физической форме», а КБ – это уже, по сути, безопасность в КП.

Беларусь и Россия, учитывая мировой нормотворческий опыт, а также созданную нормативно-правовую базу, уже сделали собственные шаги в направлении трактовки понятия КБ и определения организационно-технических мер ее обеспечения.

Например, Совет Безопасности Российской Федерации и Министерство иностранных дел Российской Федерации аргументировано предпочитают вместо термина «*кибербезопасность*» использовать формулировку «*безопасность в ИКТ-среде*» [9].

В свою очередь Совет Безопасности Республики Беларусь утвердил Концепцию [1], в котором дефиниция «*кибербезопасность*» раскрывается как «состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз». Однако сформулирована она в достаточно общем виде, а понятие «*киберпространство*» в данном нормативном правовом акте отсутствует вовсе, не вполне очевидна и взаимосвязь этих понятий.

Дать определение КП в руководящем документе такого уровня все же было необходимо, так как зарубежные страны, напомним, рассматривают его как новый театр военных действий, технологическую платформу для проведения военных операций и воздействия (атак) на информационную инфраструктуру государства.

В результате, с учетом Концепции [1] и проведенных ранее исследований проблематики [10], а также в контексте предполагаемого информационного противоборства вооруженных сил с эвентуальным противником трактовку понятия «*киберпространство*» логично представить в следующем виде – «глобальная область информационной среды, включающая в свой состав взаимозависимую совокупность информационно-технической инфраструктуры, в том числе информационные и телекоммуникационные сети и их системы, предназначенные для хранения, обработки, модификации и обмена данными (информацией)».

Полученное определение КП позволяет установить содержательную часть понятия «*кибербезопасность*» как «информационная безопасность информационно-управляющих систем с используемыми ими данными (информацией), обеспечивающая их высокую

функциональную устойчивость в условиях современного информационного противоборства» [11]. В отличие от приведенного в [1] новая трактовка данного понятия учитывает взаимосвязь с понятием «киберпространство», а также выделяет предполагаемые объекты воздействия (т.е. информационные объекты в КП) и определяет необходимый результат обеспечения их КБ и ИБ в ходе информационного противоборства.

Таким образом, использование при реализации организационно-технических мер понятия «кибербезопасность» в представленной итоговой формулировке имеет ключевое значение для обеспечения информационной и кибербезопасности инфраструктур Союзного государства, региональной безопасности в целом. В частности, вооруженными силами Беларуси и России, как гаранта военной безопасности и защиты суверенитета (в том числе информационного) в мирное и военное время, а также иными организациями и ведомствами обоих государств.

Приоритетные направления обеспечения региональной безопасности. Из изложенного стало очевидным, что КП создано, развивается и функционирует в интересах множества, в том числе антагонистических информационно-управляющих систем. При этом проблемы разграничения информационных объектов обслуживаемых систем далеки от своего разрешения.

Военно-политическое руководство ведущих зарубежных государств (США и других государств альянса НАТО) придерживается концепции «проактивной киберобороны», которая охватывает весь набор мер пассивной и активной защиты своего КП от существующих или потенциальных угроз, включая в определенные моменты воздействие на источники таких угроз за пределами своих сетей.

Для коллективного исследования и передачи опыта в соответствующих сферах, в структуре НАТО создан ряд Центров компетенций, подготовки, координации и реагирования, преимущественно вблизи Союзного государства (рис. 3).

Государство-учредитель (место расположения)	Наименование центра передового опыта (ЦПО) или организации	Год начала функционирования
 Эстония (г. Таллин)	ЦПО в области кибербезопасности НАТО	2008
 Нидерланды (г. Утрехт)	ЦПО в области обеспечения систем боевого управления и связи НАТО	2008
 Италия (г. Рим, г. Виченца)	ЦПО в области моделирования и имитации боевых действий НАТО ЦПО в области постконфликтного урегулирования НАТО	2009 2015
 Румыния (г. Орадя)	ЦПО в области агентурной разведки НАТО	2009
 Польша (г. Варшава, г. Краков)	Американо-польский центр кибернетической разведки и анализа ЦПО в области контрразведывательной деятельности НАТО	2013 2018
 Бельгия (г. Брюссель, г. Монс)	Центр реагирования на киберинциденты при штаб-квартире и штабе стратегического командования операций НАТО Центр киберопераций при штабе стратегического командования операций НАТО	2013 2021
 Латвия (г. Рига)	ЦПО в области стратегической пропаганды НАТО	2014
 Финляндия (г. Хельсинки)	Европейский ЦПО по противодействию гибридным угрозам	2017

Рисунок 3. – Центры компетенций, подготовки, координации и реагирования в информационном и киберпространстве НАТО

В условиях глобализации и трансграничности КП важной задачей для Беларуси и России становится защита информационно-управляющих систем своих вооруженных сил как основного компонента военной организации государств, использующего соответствующие объекты [12]. Это подтверждается трансформацией вооруженных сил

крупнейших технологически развитых государств, которые уделяют повышенное внимание вопросам проведения операций в КП и создают специальные структуры – киберкомандования.

Применение специальных сил и средств предполагает активные действия в самом КП в интересах достижения военных целей и влияния на развитие ситуации в нужном направлении. Такие действия одновременно нацелены на глубокое проникновение и обеспечение доступности выбранных информационных объектов.

Главными задачами таких структур стратегического уровня управления являются:

- постоянный контроль КП;
- планирование, координация, интеграция, синхронизация и управление операциями в КП;
- обеспечение ИБ и КБ не только военной и государственной инфраструктуры, но и КВИИ.

Атаки на КВИИ государства посредством КП осуществляются с использованием кибероружия. Кибероружие может применяться поэлементно, массировано и в том числе комплексно с физическими атаками против инфраструктуры и ключевых объектов государств. С помощью кибероружия возможно разрушить информационно-управляющую систему, уничтожение которой классическим оружием невозможно либо нецелесообразно (например, банковскую систему для достижения эффекта экономического коллапса). Только лишь физическое разрушение элементов систем затруднит их восстановление и дальнейшее использование, помимо этого, может быть нанесен косвенный ущерб союзникам и членам международного сообщества, не участвующим в конфликте.

Следовательно, основными целями применения кибероружия являются:

- целенаправленное изменение характеристик КП;
- дезинтеграция систем управления, обеспечения, целеуказания противника;
- захват объектов или блокирование управления объектами КП;
- перевод КВИИ противника в режим, соответствующий собственным задачам.

В итоге первоочередными задачами по защите КВИИ Союзного государства на текущий момент являются:

- разработка (синхронизация) общих государственных мер по контролю и защите собственного КП;
- уточнение целей, задач, средств и способов применения существующих структур своих вооруженных сил с учетом необходимости проведения оборонительных и наступательных операций в КП;
- обоснование задач, состава и структуры вновь создаваемых сил и средств своих вооруженных сил для проведения операций в КП;
- разработка документов, регламентирующих порядок создания и использования объектов КП в интересах своих вооруженных сил в условиях мирного и военного времени;
- разработка документов, регламентирующих порядок взаимодействия своих вооруженных сил с соответствующими организациями и ведомствами по обеспечению ИБ и КБ на КВИИ в условиях мирного и военного времени.

Таким образом, информационная и кибербезопасность инфраструктур Союзного государства в настоящее время связана с необходимостью концентрации совместных усилий организаций и ведомств различного уровня и подчиненности/принадлежности на предотвращение экзистенциальных кибератак против национальных информационных объектов в киберпространстве. Данный формат реализации организационно-технических мер информационной и кибербезопасности инфраструктур является ключевым фактором обеспечения региональной безопасности, наряду с коалиционной безопасностью государств – членов Организации Договора о коллективной безопасности, и служит общим интересам Беларуси и России в других сферах [13, 14].

Заключение

Национальная нормативно-правовая база государств Союза Беларуси и России в области обеспечения безопасности собственного информационного и киберпространства

требует дальнейшей корректировки и синхронизации. В частности, понятие «киберпространство» нормативно не закреплено, различаются подходы к трактованию и использованию дефиниции «кибербезопасность», что накладывает свой отпечаток на определение организационно-технических мер ее обеспечения. Некоторые несоответствия отмечаются и в законодательстве других государств, при составлении словарей и военно-политических документов, а также в практике международной стандартизации.

По результатам проведенных исследований автором предложена собственная формулировка дефиниции «кибербезопасность», которая учитывает взаимосвязь с понятием «киберпространство». Использование ее в таком ключе позволит реализовать адекватные организационно-технические меры обеспечения информационной и кибербезопасности инфраструктур Союзного государства, региональной безопасности в целом.

В условиях глобализации и трансграничности киберпространства важной задачей для Беларуси и России становится защита информационно-управляющих систем своих вооруженных сил как основного компонента военной организации государств, использующего соответствующие объекты в мирное и военное время. Так как, следуя мировым тенденциям, вооруженные силы Союзного государства должны предпринимать проактивные действия для обеспечения информационной и кибербезопасности национальных инфраструктур. Их результаты будут составлять большую часть общих усилий организаций и ведомств различного уровня и подчиненности/принадлежности по предотвращению экзистенциальных кибератак против национальных информационных объектов в киберпространстве.

Литература

1. Концепция информационной безопасности Республики Беларусь [Электронный ресурс]: пост. Сов. безоп. Респ. Беларусь, 18 марта 2019 г., № 1 // Нац. правовой Интернет-портал Респ. Беларусь. – Режим доступа: https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf. – Дата доступа: 20.04.2023.
2. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // Российская газета. – Режим доступа: <https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html>. – Дата доступа: 20.04.2023.
3. Указ Президента Республики Беларусь № 40 «О кибербезопасности» [Электронный ресурс] // Офиц. сайт Президента Респ. Беларусь. – Режим доступа: <https://president.gov.by/bucket/assets/uploads/documents/2023/40uk.pdf>. – Дата доступа: 20.04.2023.
4. Центр ГосСОПКА [Электронный ресурс] – Режим доступа: <https://g-sopka.ru>. – Дата доступа: 20.04.2023.
5. Moller, D.P.F. Cybersecurity in Digital Transformation / D.P.F. Moller // Scope and Applications. – Springer, 2020. – 126 p.
6. Архипова, Е.А. Современное понимание терминов «кибернетическая безопасность» и «информационная безопасность» / Е.А. Архипова // Young Scientist. – 2019. – № 12 (76). – С. 315–320.
7. The NATO Cooperative Cyber Defence Centre of Excellence [Электронный ресурс]. – Режим доступа: <https://ccdcoe.org/>. – Дата доступа: 20.04.2023.
8. Wilson, D.C. Cybersecurity. / D.C. Wilson. – MIT, 2021. – 160 p.
9. Крутских, А.В. Международная информационная безопасность: теория и практика / А.В. Крутских, А.В. Бирюков, С.М. Бойко, С.Г. Волкова, Е.С. Зиновьева, А.В. Зинченко, Д.В. Матюхин, А.И. Смирнов // Учебник для вузов: в 3 томах / Под общ. ред. А.В. Крутских. – М.: МГИМО, 2021. – Том 1 (2-е изд., доп.). – 384 с.
10. Бородакий, Ю.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Ч. 1) / Ю.В. Бородакий, А.Ю. Добродеев, И.В. Бутусов // Вопросы кибербезопасности. – 2013. – № 1 (1). – С. 2–9.
11. Федорцов, А.В. Концептуальные положения кибербезопасности Вооруженных Сил / А.В. Федорцов // Прикл. аспекты науч. деятел. в обл. обор. и безоп. гос.: 20-летний опыт НИИ Вооруженных Сил: матер. V Междунар. науч.-техн. (практ.) конф., Минск,

25–26 мая 2022 г. / Науч.-исслед. ин-т Вооруженных Сил Респ. Беларусь; редкол.: В.А. Тумар [и др.]. – Минск, 2022. – С. 81–85.

12. Гнилозуб, В.В. Основы обеспечения кибербезопасности Вооруженных Сил Республики Беларусь / В.В. Гнилозуб, И.Н. Сафроняк, А.В. Федорцов // Наука и воен. безопасность. – 2021. – № 4 (70). – С. 2–8.

13. Федорцов, А.В. Основы коалиционной безопасности информационного и киберпространства государств-членов ОДКБ / А.В. Федорцов // Развиг., подгот. и примен. сил и средств сист. коллектив. безоп. Организации Договора о коллектив. безоп.: матер. Междунар. воен.-науч. конф., Минск, 16–17 ноября 2022 г. / Науч.-исслед. ин-т Вооруженных Сил Респ. Беларусь; редкол.: В.А. Тумар [и др.]. – Минск, 2022. – С. 124–126.

14. Военная доктрина Союзного государства [Электронный ресурс] // Правовой портал Союзного государства. – Режим доступа: <https://посткомсг.рф/documentation/document/1899>. – Дата доступа: 20.04.2023.

РАЗРАБОТКА МЕТОДА ВЫЯВЛЕНИЯ ИНФОРМАЦИОННОГО ВЛИЯНИЯ В СОЦИАЛЬНЫХ СЕТЯХ

А.Е. КАРЕТНИКОВ, А.В. ЧУВАЕВ

*МИРЭА – Российский технологический университет,
г. Москва, Россия*

Введение

Миллионы пользователей каждый день пользуются социальными сетями: отправляют сообщения друзьям, читают ленту новостей и т.п. С одной стороны, все это приносит людям очевидную пользу, с другой – социальные сети стали эффективным инструментом влияния на поведение большого числа людей. Не для кого ни секрет, что с их помощью преступные сообщества, в том числе террористические и экстремистские движения, вовлекают в свои ряды новых участников [1, 2] и, а также оказывают деструктивное воздействие [3]. Это воздействие носит характер информационных волн, вызываемых определенными информационными поводами, информация о которых вбрасывается в социальную сеть и имеет цель охватить максимальное количество пользователей.

Социальные сети постоянно развиваются, а вместе с этим также совершенствуются и методы деструктивного влияния на пользователей, в результате чего необходимо постоянно совершенствовать существующие методы выявления подобных воздействий и имеющиеся методы противоборства.

1. Преимущества предлагаемого метода

Данная работа предлагает за основу разрабатываемого метода выявления информационного влияния взять метрику «центральность по степени» [4], поскольку она лишена большинства недостатков других подходов [5, 6]:

- недостатка, связанного с вычислительной сложностью;
- отсутствует необходимость наличия информации обо всех субъектах сети;
- она может рассчитываться на основе произвольных характеристик и связей субъекта.

Последний пункт позволяет выбрать такие характеристики субъекта для подсчета данной метрики, информация о которых:

- во-первых, будет всегда общедоступной, несмотря на тенденцию к усилению приватности, иначе потеряется смысл социальной сети. Это позволит избежать необходимость корректировки разрабатываемого метода в будущем;
- во-вторых, данный выбор может существенно сказаться на релевантности применения метрики. Таким образом, имеется возможность устранить ее основной недостаток, связанный с плохой релевантностью.

Соответственно, необходимо определить характеристики, удовлетворяющие рассмотренным выше условиям, на основе которых будет рассчитываться метрика. Учитывая, что публикации пользователей, а также их комментарии в социальных сетях по большей части представлены в виде текста, а именно в этом тексте содержится информационный посыл, который направлен на других пользователей, при определении информационного влияния имеет смысл анализировать то, что пишут пользователи. Извлеченная из публикаций информация позволит строить гораздо больше выводов о пользователе, а следовательно, и в целом о его информационном влиянии на социальную сеть. Кроме того, в последние годы развитие алгоритмов машинного обучения и сферы искусственного интеллекта происходит весьма интенсивно, достигнуты значимые практические результаты: разработанные алгоритмы и их реализации в библиотеках существующих языков программирования позволяют создавать приложения, которые достаточно эффективно распознают естественный язык и позволяют решать различные задачи, связанные с его обработкой:

- классификация текстов по темам;
- распознавание именованных сущностей – извлечение из текста такой информации, как имена людей, названия географических объектов, названия организаций;

- анализ тональности – классификация текстов по их эмоциональному послылу.

В текущей работе предлагается воспользоваться данными достижениями в области искусственного интеллекта. Актуальность использования такого выбора повышается тем, что существующие подходы не рассматривают семантической составляющей публикаций пользователей.

2. Описание алгоритма

Итак, перейдем к определению метрики, позволяющей находить источники информационного влияния в социальных сетях. Ключевыми источниками информационного влияния являются пользователи. Своим массовым воздействием на других пользователей они могут оказывать двумя способами – публикацией различных записей, а также комментированием чужих записей. Поскольку записи зачастую не имеют конкретных авторов, а публикуются от имени сообщества, например, от имени новостного агентства, наибольший интерес представляет рассмотрение комментариев различных пользователей. Поэтому в качестве метрики предлагается рассматривать число комментариев у пользователя, но с целью повышения релевантности поиска не всех, а на определенную тему, определенной тональности, с упоминанием определенных именованных сущностей. Кроме того, также предлагается учитывать наличие схожих комментариев как у одного автора, так и у различных пользователей. Логично предположить, что отдельное деструктивное информационное воздействие, направленное на искажение и изменение представлений других пользователей, будет иметь конкретную цель, касаться определенного представления, которое будет описываться определенной тематикой текста, определенным набором упоминаемых в нем именованных сущностей (некоторым контекстом), а оказываться оно будет набором схожих эмоциональных комментариев. Все это позволит аналитику не просто выявлять случаи информационных воздействий, но также задавать различные параметры, такие как интересующие события, тональность, пороги чувствительности метрики. Этапы предлагаемого метода показаны на рисунке 1.

На первом этапе происходит сбор информации о публикациях в социальной сети, комментариях к ним, а также авторах этих комментариев (достаточно минимальной общедоступной информации, чтобы понимать, от имени какого пользователя выполняется комментирование).

Далее анализируются публикации, определяются их темы, встречающиеся в них именованные сущности (люди, организации, географические названия), выполняется поиск похожих публикаций. В данном случае анализ тональности не представляет интерес, поскольку в данной работе предлагается рассматривать крупные новостные сообщества и публикации, осуществляемые от их имени. Как правило, они придерживаются нейтральной тональности.

На следующем этапе анализируются комментарии, здесь уже определение тональности играет важную роль, поскольку они пишутся непосредственно от имени пользователей и, как правило, имеют эмоциональную окраску. Особенно в случае желания оказать воздействие на наибольшее количество пользователей. Также определяются схожие комментарии. Извлекать сущности и определять тему комментария не имеет смысла, поскольку это достаточно короткие сообщения. Гораздо удобнее определять тематику комментария по теме комментируемой публикации, а также контексту упоминаемых в ней сущностей.

На заключительном этапе происходит вычисление метрики, которая будет выражать наличие деструктивного информационного влияния от пользователя.



Рисунок 1. – Этапы предлагаемого метода выявления информационного влияния

3. Определение метрики

Метрика содержит три компонента. Введем следующие обозначения:

- C – множество всех комментариев;
- U – множество всех пользователей;
- T – множество всех тем публикаций;
- N – множество всех именованных сущностей;
- E – множество всевозможных контекстов, элемент данного множества задается темой публикации, а также набором встречаемых в ней сущностей: $e \in E \Rightarrow e = \{t, n_1, \dots, n_m\}, t \in T, n_1, \dots, n_m \in N$. В случае, когда $e = \emptyset$ будем говорить о том, что контекст не определен;

• $\alpha(c) = u, c \in C, u \in U$ – функция, которая ставит в соответствие комментарий c его автора u ;

• $s(c_1, c_2) \in [0, 1], c_1, c_2 \in C$ – оценка сходства двух комментариев, принимающая значение в диапазоне от 0 до 1. В случае 0 – различные комментарии, 1 – одинаковые комментарии;

• $t(c) \in [-1, 1], c \in C$ – оценка тональности комментария, принимающая значение в диапазоне от -1 до 1. В случае -1 – комментарий имеет негативную тональность, 1 – комментарий имеет позитивную тональность;

• $\sigma(c) = e, c \in C, e \in E$ – функция, которая ставит в соответствие комментарий c его контекст e .

Каждый пользователь u и его комментарий c могут быть охарактеризованы следующими компонентами предлагаемой метрики влияния M относительно некоторого контекста e :

- количеством негативных комментариев, связанных с данным контекстом:

$$A = |\{c_i \mid c_i \in C, \alpha(c_i) = u, \sigma(c_i) = e, t(c_i) < -0,5\}|;$$

- количеством схожих комментариев, связанных с данным контекстом:

$$I = |\{c_i \mid c_i \in C, \alpha(c_i) = u, \sigma(c_i) = e, s(c, c_i) \geq 0,75\}|;$$

- количеством авторов, пишущих схожие комментарии, связанные с данным контекстом:

$$O = |\{u_i \mid u_i \in U, \exists c_i \in C: \alpha(c_i) = u_i, s(c, c_i) \geq 0,75, \sigma(c) = e\}|.$$

Имеем, $M = \{A, I, O\}$. Говорить о вероятном оказании деструктивного информационного воздействия можно в случаях, когда фиксируется превышение пороговых значений, которые можно задавать произвольно, ниже приводятся некоторые рекомендации:

- $A \geq \mu$. Выбор порога μ в данном случае зависит от величины рассматриваемого временного периода. Для нескольких (1–3) дней предельным значением может являться наличие более 10 негативных комментариев;

- $I \geq \gamma$. Выбор порога γ также зависит от величины рассматриваемого периода, а также тональности исходного комментария. Для негативных комментариев и нескольких (1–3) дней значением данного порога может служить наличие хотя бы трех одинаковых негативных комментариев, в случае нейтральной тональности – более 10;

- $O \geq \lambda$. В данном случае в любом случае в качестве λ можно выбрать минимальное наличие 2-3 авторов, поскольку вероятность случайного совпадения комментариев у разных авторов крайне мала.

Литература

1. «Концепция об обеспечении международной информационной безопасности (концепция)», Министерство иностранных дел Российской Федерации, 2011 Сентябрь 22. [В Интернете]. Available: https://www.mid.ru/ru/foreign_policy/official_documents/1698725/. [Дата обращения: 28 Апрель 2023].

2. «Использование Интернета в террористических целях», Организация Объединенных Наций, Нью-Йорк, 2013.

3. «Указ Президента Российской Федерации от 12.04.2021 г. № 213 "Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности",» Президент России, [В Интернете]. Available: <http://www.kremlin.ru/acts/bank/46614>. [Дата обращения: 28 Апрель 2023].

4. L.C. Freeman, «Centrality in Social Networks Conceptual Clarification» *Social Networks*, № 1, pp. 215–239, 1978.

5. А.Н. Рабчевский, «Методы и алгоритмы поддержки принятия решений по противодействию деструктивным воздействиям в социальных сетях» Пермский государственный национальный исследовательский университет, 2022.

6. Д.А. Губанов и А.Г. Чхартишвили, «Влиятельность пользователей и метапользователей социальной сети» Управление в социально-экономических системах, 2016.

ЗАСЕДАНИЕ № 3

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ

УДК 004.056

ФИЛОСОФИЯ БЕЗОПАСНОСТИ КИБЕРПРОСТРАНСТВА

М.Н. БОБОВ

*Учреждение образования БГУИР, каф. ИКТ, ф-т защиты информации,
г. Минск, Республика Беларусь*

Введение

С появлением в последнюю треть XX столетия сложных цифровых технологий сетевых коммуникаций и их объединения и интегрирования с вычислительными ресурсами и информационными системами, сети стали основной формой организации и взаимодействия социальных, политических и экономических сил. Это привело к появлению искусственного пространства глобального масштаба – киберпространства, которое прочно вошло в жизнь современного человека. С распространением в начале 1990-х гг. Всемирной паутины (*World Wide Web, WWW*) термин «киберпространство» получил практическое применение для описания онлайн-мира, в котором взаимодействия индивидов и групп осуществляются посредством электронных сетей, соединенных средствами информационно-коммуникационных технологий. Несмотря на то что вот уже на протяжении 30 лет вокруг киберпространства ведутся активные дискуссии, однозначной трактовки этого понятия нет до сих пор, а в большинстве социологических справочников этот термин отсутствует.

Вместе с тем киберпространство, или по-другому цифровая среда, – это пространство функционирования продуктов информационно-коммуникационных технологий, позволяющих создавать чрезвычайно сложные системы взаимодействий агентов с целью получения информации, обмена и управления ею, а также осуществления коммуникаций в условиях множества различных сетей [1].

2. Ключевые характеристики киберпространства

Первой отличительной характеристикой киберпространства является его виртуальность. Это означает, что киберпространство жестко не привязано и не зависит от конкретного пространственно-временного расположения. Место взаимодействия в киберпространстве не требует, чтобы агенты взаимодействия находились в одном конкретном месте в определенный момент времени для того, чтобы их встреча в киберпространстве состоялась. Несомненно, взаимодействие в киберпространстве обеспечивается физической средой, но оно может быть синхронным или асинхронным и может быть доступно агентам практически в любом географическом пространстве. Виртуальность здесь не выступает противоположностью действительности. Тем не менее виртуальность обозначает то, что нечто в киберпространстве может быть совсем не тем, чем кажется. Таким образом, киберпространство, будучи виртуальной средой, не является физическим местом в привычном смысле, когда площадка или пространство для взаимодействия ограничено пространственно-временными рамками.

Другой важной характеристикой киберпространства является связь между киберпространством и сетью. Киберпространство нельзя отождествлять с сетью или описывать как совокупность данных, хранящихся на компьютерах, и предоставляемых через компьютерные сети. Однако киберпространство во многом зависит от функционирования информационно-коммуникационных сетей (преимущественно речь идет об интернете). Конкретизируя, можно сказать, что киберпространство является пространством, которое контролирует существование и работу взаимосвязанных сетей компьютеров. Следовательно, любое изменение состояния соответствующих взаимосвязанных компьютеров, также будет связано с изменением взаимодействия в киберпространстве.

Третьей характерной чертой киберпространства является его размытость и неопределенность границ. По аналогии с сетью, киберпространство в этом случае характеризуется децентрализацией и не является четко определенным и заданным. Вместе с тем оно выступает как пространство для взаимодействия, создавая множество связей сетевой структуры, а также полей для взаимодействий в рамках различных сообществ с бесконечным числом вариантов индивидуальной репрезентации. [2]

3. Риски киберпространства

Являясь чрезвычайно подвижной и гибкой, среда киберпространства не только создает бесконечное число новых возможностей, но и порождает новые риски, с которыми человечество никогда ранее не сталкивалось, а именно:

- проявление киберпреступности против личности, государства, общества;
- сращивание национальной и зарубежной преступности в транснациональные преступные синдикаты;
- информационный вандализм и хакерство;
- информационный терроризм на внутригосударственном и международном уровнях;
- информационные войны на внутригосударственном и международном уровнях, которые способны вызвать взрывы на химических заводах и токсичные облака над мегаполисами, пожары на нефтехранилищах и трубопроводах, транспортный коллапс на дорогах и в аэропортах, а нация оказывается буквально парализована без электричества, управления, защиты и информации о том, что происходит [3].

Указанные риски обусловлены самой сутью киберпространства, которое является полем функционирования экономических институтов и отражает современное объективно существующее социальное неравенство. Ограниченный доступ в зависимости от уровня дохода, образования, пола, возраста, происхождения, расы или языка демонстрирует цифровой разрыв, существующий в современном мире как на глобальном уровне, так и на уровне отдельных государств. Поэтому на повестке дня остро стоят вопросы безопасности киберпространства, перспективы развития «цифровой» экономики и «цифровой» культуры общества. Человечество стало заложником собственноручно созданных технологий. Теперь существование этих технологий является основой стабильного функционирования общества информационной эпохи господства сетевых структур [4].

4. Философия безопасности киберпространства

В связи с необходимостью обеспечения безопасности киберпространства возникает вопрос, «Возможно ли органичное сочетание использования сверхсовременных технологий с традиционными духовными ценностями и идеалами человечества?» Именно поэтому в 2012 г. был опубликован международный стандарт ISO/IEC 27032 «Наставления по кибербезопасности», разработанный Подкомитетом № 27(SC27) по информационной безопасности Первого объединенного технического комитета (JTC1) ISO/IEC [5].

Безопасность и стабильность Киберпространства во многом зависит от безопасности и надежности входящих в него сегментов критической инфраструктуры и тесно связана с безопасностью Интернет, промышленных, частных и домашних компьютерных сетей, а также с информационной безопасностью в целом.

Нужно отметить, что доменам безопасности, названным выше, присущи свои специфические особенности, цели и задачи. Поэтому решение вопросов обеспечения кибербезопасности требует плотного взаимодействия различных структур: частных и государственных, в том числе на уровне взаимодействия стран и международных организаций. Однако, правительства разных стран зачастую относят свои объекты критической инфраструктуры к сфере интересов национальной безопасности, поэтому, исключают возможность их открытого обсуждения, понимая, что раскрытие сведений об их уязвимости может прямо повлиять на общее состояние национальной безопасности [6]. При разрешении проблем, обусловленных объективным наличием недоступных участков получения соответствующих гарантий, провайдерам и потребителям

необходимо координировать свои усилия и придерживаться общих схем распространения и совместного использования информации.

Оказалось, что в зонах пересечения информационной безопасности, интернет-безопасности, сетевой безопасности и ИКТ-безопасности, составляющих основу безопасности киберпространства, обнаруживаются неизвестные ранее явления и возникают проблемы, преодолеть которых невозможно на основе имевшегося ранее опыта решения задач безопасности и существовавшей практики взаимодействия провайдеров и потребителей. Причина кроется в большом числе владельцев оборудования и сетей телекоммуникаций, каждый из которых исповедует свою логику бизнеса и собственное видение текущей ситуации. Каждый из провайдеров и каждый из потребителей преследуют свои собственные интересы безопасности в Киберпространстве, и даже минимальное переключение взаимодействия с одного провайдера или потребителя на другого может оказать существенное влияние на монолитность и однородность безопасности киберпространства в целом.

5. Структура наставления по кибербезопасности

Первой зоной внимания Стандарта объявляются проблемы, обусловленные разрывами между различными доменами безопасности Киберпространства (т.е. кибербезопасности). В частности, Стандарт признает наиболее распространенными следующие угрозы:

- атаки социального инжиниринга;
- хакинг;
- эпидемии компьютерных вирусов (“malware”);
- внедрение шпионских программ;
- действие прочих нежелательных программных кодов.

Технические рекомендации в отношении обращения с рисками реализации названных угроз, включают меры:

- готовности к отражению атак со стороны:
 - а) автономных вредоносных кодов,
 - б) отдельных злоумышленников,
 - в) преступных и агрессивных организаций в Интернет;
- обнаружения и мониторинга атак;
- подавления атак.

Поскольку в Киберпространстве необходимо не только действенно и эффективно распространять информацию среди провайдеров и потребителей, но и координировать их совместные усилия в их объединенной реакции на инциденты, постольку второй зоной внимания Стандарта являются аспекты взаимодействия. Взаимодействие должно осуществляться на основе обеспечения взаимной безопасности и надежности, а также взаимного признания и уважения информационного суверенитета каждого из стейкхолдеров, в частности, с пониманием того, что разные стейкхолдеры могут находиться в географически различных регионах, часовых поясах и относиться к различным юрисдикциям.

В связи с этим в Стандарте приведены общие рекомендации в отношении:

- совместного использования информации,
- координации,
- обработки инцидентов.

Приведенные рекомендации касаются:

ключевых элементов, которые необходимо учитывать при назначении прав допуска, обязательных процедур при взаимодействии, обмене информацией и ее совместном использовании;

формальных требований взаимодействия стейкхолдеров и технических условий, выполнение которых необходимо для интеграции технических систем.

Рекомендации Стандарта ориентированы на руководителей высшего уровня, тогда как детальные технические спецификации и рекомендации, ориентированные на конкретные применения, содержатся в источниках, ссылки на которые приведены в тексте Стандарта. Разработанный Стандарт представляет собой руководство по повышению уровня

кибербезопасности в контексте ее уникальности и непересечения с другими доменами безопасности, а именно, такими как:

- информационная безопасность;
- безопасность частных сетей;
- интернет-безопасность;
- безопасность инфраструктуры.

В Стандарте изложены основные рекомендации по обеспечению безопасности ключевых информационных систем объектов критической инфраструктуры и физических лиц в Киберпространстве, в том числе:

- обзор общих сведений по кибербезопасности;
- позиционирование кибербезопасности по отношению к другим доменам безопасности;
- определение ролей стейкхолдеров в обеспечении кибербезопасности;
- рекомендации в отношении решения общих проблем кибербезопасности;
- общие принципы информационного взаимодействия и обмена информацией в процессе разрешения проблем кибербезопасности.

6. Проблемы обеспечения безопасности киберпространства

Вместе с тем, стандарт ИСО/МЭК 27032 не решает многих проблем, связанных с обеспечением безопасности киберпространства.

Во-первых, необходимо учитывать, что киберпространство – это особый вид пространства, которому присущи ряд специфических свойств, а именно:

- виртуальность;
- неделимость, несводимость к границам физического пространства;
- отсутствие однозначной географической определенности;
- многомерность и отсутствие линейности, протяженности, физических параметров;
- подвижность и изменчивость.

Во-вторых, в основе киберпространства лежит Интернет, протоколы взаимодействия которого создавались в течение не менее 30 лет, не лишены изъянов и требуют обновления.

Ответ на вопрос: «Обеспечивает ли киберпространство безопасность физических активов, которые существуют в реальном мире в материальной форме и виртуальных активов, которые существуют только в Киберпространстве от угроз, вызывающих риски, сформулированные ранее в разделе 3?» лежит, на наш взгляд, в плоскости философии науки и техники и должен решаться путем определения местоположения киберпространства в той философской картине мира, в которой нуждается современная цивилизация.

Рассмотрение философии безопасности киберпространства, таким образом, следует проводить в русле основных частей философии науки и техники, к которым относятся [7]:

- онтология – учение о бытии;
- гносеология – учение о познании;
- диалектика – учение о развитии
- аксиология (теория ценностей);
- герменевтика (теория понимания и толкования знаний).

Наиболее важными (первостепенными) для философского определения и исследования безопасности киберпространства являются онтология и диалектика. Определим основные направления в области онтологии и диалектики, которые необходимо рассмотреть для создания целостной системы безопасности киберпространства, обеспечивающей по определению конфиденциальность, целостность и доступность защищаемой информации.

6.1 Направления исследований в части онтологии безопасности

Ранее философский термин «онтология» означал учение о бытии, затем он переместился в область точных наук, где полуформализованные концептуальные модели всегда сопутствовали математически строгим определениям. Под определение онтологии подпадают многие понятийные структуры: иерархия классов в объектно-ориентированном

программировании, концептуальные карты (concept maps), семантические сети, и т.п. Представляется, что онтологию можно трактовать еще шире – например, как сценарий или процесс, как нечто структурирующее хаос. Приведем современное определение онтологии, приведенное в [8].

Онтология – это структурная спецификация некоторой предметной области, ее формализованное представление, которое включает словарь (или имена) указателей на термины предметной области и логические выражения, которые описывают, как они соотносятся друг с другом.

6.1.1. Алгоритм онтологического инжиниринга, как правило, включает в себя выполнение следующих этапов:

- выделение концептов – базовых понятий характерных для обеспечения безопасности киберпространства;
- определение «высоты дерева онтологий» – числа уровней абстракции, необходимых для описания среды безопасности;
- распределение концептов безопасности по уровням;
- построение связей между концептами – определение отношений и взаимодействий базовых понятий необходимых для создания системы безопасности киберпространства;
- консультации со специалистами различных областей знаний для исключения противоречий и неточностей.

6.1.2. Инжиниринг онтологий базируется на использовании следующих инструментов:

- когнитивные принципы формирования онтологий;
- языки формализации онтологий;
- инструментальные интегрированные среды инжиниринга онтологий;
- конструирование онтологий;
- нахождение семантических связей, подобия между онтологиями;
- композиция онтологий;
- динамика онтологий и денотативных баз данных;
- платформы, форматы, стандарты для инжиниринга онтологий;
- экспертные системы, оболочки и компоненты.

6.1.3. Должна быть разработана онтология проектирования системы безопасности киберпространства как научное направление, которое включает в себя:

- 1) исследование понятийного аппарата и разработки на его основе тезауруса, анализ критериев и моделей проектируемой системы безопасности;
- 2) разработку методов и сценариев проектирования, сбор и обработку информации об объектах как элементах системы и о составляющих компонентах объектов;
- 3) онтологию проектирования системы безопасности, ее понятийный аппарат и базовые принципы безопасности киберпространства в целом и каждой из составляющих его предметных областей;
- 4) обобщение и накопление опыта из разных предметных областей, структуризацию знаний об объектах и методах проектирования, разработка совокупности семантических справочников, баз данных и процедур, алгоритмов оптимизации и учета проектной неопределенности.
- 5) создание формализованного описания знаний субъектов проектирования о процессе проектирования новых или модернизации уже известных систем безопасности, включая знания о самом объекте проектирования и близких к нему по свойствам систем.

В результате исследований онтологии системы безопасности киберпространства должны быть получены:

- принципы использования онтологий в проектировании системы безопасности киберпространства;
- проектирование системы безопасности киберпространства, управляемое онтологией и использующее онтологий;
- параллельное проектирование систем безопасности;

онтологии безопасности предметных областей проектирования;
интеллектуальные системы проектирования, использующие онтологии;
технические справочники на основе онтологий;
онтологии проектирования и обучающие системы;
тезаурусы и базы знаний в проектировании системы безопасности киберпространства.

6.2. Направления исследований безопасности киберпространства с позиций диалектики

В современной философии диалектика предстает в виде теории развития бытия и метода его познания. Диалектический метод необходим ученым не потому, что так кому-то очень хочется, а потому, что в конечном счете в природе, обществе и в самом человеческом мышлении все свершается диалектически, поэтому диалектический метод – это путь к научному познанию. Структуру диалектики как теоретической системы образуют принципы, законы и категории.

К основным принципам диалектики относятся:

- принцип развития;
- принцип всеобщей связи.

Принцип развития фиксирует динамику всех вещей и явлений реальности, а принцип всеобщей связи характеризует отношения зависимости, существующие в мире между вещами, явлениями, их свойствами. Связи, которые носят общий, существенный, необходимый и устойчивый характер, в диалектике называют законами. Традиционно законы диалектики подразделяют на основные и неосновные. Основные законы диалектики раскрывают сущность развития, а дополнительные – дополняют картину развития [9].

6.2.1. Основные законы диалектики включают в себя:

- 1) закон единства и взаимодействия противоположностей, или закон противоречия;
- 2) закон перехода количественных и качественных изменений;
- 3) закон отрицания отрицания.

В современном научном познании диалектико-материалистический метод играет возрастающую роль, поскольку он функционирует не в виде жесткой и однозначной совокупности норм, рецептов, а в качестве гибкой диалектической системы всеобщих принципов и является регулятором человеческой деятельности, в том числе мышления.

Диалектический метод дает способ реконструкции развития объекта и реализуется путем выполнения следующих этапов.

1. Определение внутренних противоречий любой системы являющихся главным источником, обуславливающим причину ее развития.
2. Выделение среди множества противоречий системы ее основного противоречия.
3. Полагание неразвитой, простейшей по содержанию (и благодаря этому всеобщей) формы основного противоречия в качестве исходного начала всего последующего процесса рациональной реконструкции развития изучаемой системы.
4. Определение в виде диалектической цепочки: тезис – антитезис – синтез всех остальных вытекающих противоречий путем последовательного развертывания исходного (абстрактного) противоречия.
5. Многократное повторение синтеза каждого из выделенных противоречий для реализации его на более высоком конкретном уровне.

6.2.2. Диалектический метод опирается на следующие принципы:

- 1) **объективность**, представленная в следующих требованиях: а) исходит из практики; б) реализует активную роль субъекта познания; в) умение выразить логику вещей в логике понятий; г) умение выбрать адекватную систему методов; д) рассматривать объект в социокультурном контексте; е) подходить к процессам конструктивно-критическим; ж) действовать в соответствии с логикой данного предмета;

2) **всесторонность**, опирающаяся на признание всеобщей связи явлений действительности и основанная на требованиях: а) вычлениении предмета исследования и проведение его границ; б) целостное и многоаспектное рассмотрение; в) изучение в чистом

виде каждой из сторон предмета; г) развертывание исследования вглубь и вширь; д) вычленение сущности, главной стороны субъекта и его субстанционального свойства;

3) **конкретность**, основанная на требованиях: а) создание идеальной модели явления в виде расчлененного целого; б) рассмотрение общего в единичном, сущности в явлениях, закона в его модификациях; в) учет места, времени и других обстоятельств, изменяющих бытие предмета; г) рассмотрение предмета в составе более широкого целого;

5) **противоречивость**, основанная на следующих требованиях: а) выявление внутренних и внешних противоречий изучаемого явления; б) анализ каждой из противоположных сторон; в) рассмотрение явления как единства противоположностей в целом; г) определение места отдельного противоречия в системе других противоречий; д) анализ этапов развития этого противоречия; е) исследование механизма исследования противоречия как процесса его развертывания и обострения. Неверная реализация применения принципов противоречия приводит к объективизму и субъективизму, которые могут выражаться в эклектике, в софистике или в заблуждениях.

Анализ нормативных документов РФ, изложенных в Указах в Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» и «Об утверждении доктрины информационной безопасности Российской Федерации» [10, 11] показывает, что в них закреплены характерные признаки киберпространства, определено его место в информационной сфере, а также предложено решение вопроса об установлении юрисдикции в отношении определенного сегмента киберпространства. Юрисдикция государства распространяется как на физический, материальный аспект киберпространства, представляющий собой определенную технологическую инфраструктуру (объекты информатизации, технические средства), так и на информацию в цифровой форме. Включение в информационную инфраструктуру РФ совокупности объектов информатизации, информационных систем, сетей связи, а также лишенных географических границ и пространственной протяженности сайтов в сети Интернет, позволяет заключить, что в Доктрине информационной безопасности РФ предпринята попытка «территориализации» определенного сегмента киберпространства в целях распространения на него юрисдикции государства [12]. При этом следует заметить, что понятие «киберпространство» по сравнению с понятием «сеть Интернет» включает в себя более широкий контур сетей связи, что обуславливает необходимость пополнения законодательного тезауруса данным термином, а также решения правового вопроса относительно очерчивания юрисдикции государства в отношении того или иного сегмента киберпространства. При этом игнорируется определенная материальная база его функционирования, которой может являться та или иная технологическая инфраструктура в виде специального оборудования, сервера, компьютеров и др.

Заключение

1. В связи с необходимостью обеспечения безопасности киберпространства в 2012 г. был опубликован международный стандарт ISO/IEC 27032 «Наставления по кибербезопасности», разработанный Подкомитетом № 27(SC27) по информационной безопасности Первого объединенного технического комитета (JTC1) ISO/IEC.

2. Разработанный Стандарт представляет собой руководство по повышению уровня кибербезопасности в контексте ее уникальности и пересечения с доменами безопасности, включающими: информационная безопасность, безопасность частных сетей, интернет-безопасность и безопасность инфраструктуры.

3. Вместе с тем, стандарт ИСО/МЭК 27032 не решает многих проблем, связанных с обеспечением безопасности киберпространства. Ответ на вопрос: лежит, на наш взгляд, в плоскости философии науки и техники и должен решаться путем определения местоположения киберпространства в той философской картине мира, в которой нуждается современная цивилизация.

4. Наиболее важными (первостепенными) для философского определения и исследования безопасности киберпространства следует проводить в русле основных частей

философии науки и техники, к которым относятся: онтология и диалектика, которые необходимо рассмотреть для создания целостной системы безопасности киберпространства, обеспечивающей по определению конфиденциальность, целостность и доступность защищаемой информации.

5. Анализ нормативных документов РФ, изложенных в Указах в Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» и «Об утверждении доктрины информационной безопасности Российской Федерации» показывает, что в них закреплены характерные признаки киберпространства, определено его место в информационной сфере, а также предложено решение вопроса об установлении юрисдикции в отношении определенного сегмента киберпространства.

Литература

1. Лефевр А. Производство пространства. М., 2015. – С.45
2. Мигулева М.В. Киберпространство как социальный институт: признаки, функции, характеристики // Научный журнал «Дискус-Пи», 2020. – № 4 (41).
3. Добринская Д.Е. Киберпространство: территория современной жизни // Вестник Московского Университета. Сер. 18. Социология и политология, 2018. – Т. 24, № 1. – С. 52–70.
4. Федотов М.А. Конституционные ответы на вызовы киберпространства // Lex Russica, 2016. – № 3. – С. 164–182.
5. ISO/IEC 27032:2012 – Information technology – Security techniques – Guidelines for cybersecurity.
6. Ансельмо Э.Л. Киберпространство в международном законодательстве: опровергает ли развитие Интернета принцип территориальности в международном праве? // Экономические стратегии. 2006, – Т. 8, № 2. – С. 24–31.
7. К.Н. Хабибулин, В.Б. Коробков, А.А. Луговой, А.В. Тонконогов. Философия науки и техники. Цикл лекций для адъюнктов и аспирантов. – М., 2008.
8. Деннет Д. Онтологическая проблема сознания. – В кн.: Аналитическая философия: становление и развитие. М., 1998;
9. Диалектика как теория и метод познания. Философия. Учебник / Под ред. Г.В. Андрейченко, В.Д. Грачева. – Ставрополь: Изд-во СГУ, 2001.
10. Указ Президента РФ от 09.05.2017 г. № 203.
11. Указ Президента РФ от 05.12.2016 г. № 646.
12. Неманья Никитович. Стратегия и тактика кибервойн: в ожидании серьезных межгосударственных конфликтов // Information Security / Информационная безопасность, 2013. – № 5.

ОСОБЕННОСТИ ПРЕДУПРЕЖДЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Д.Н. ЛАХТИКОВ

*Учреждение образования «Академия Министерства внутренних дел Республики Беларусь»,
г. Минск, Республика Беларусь*

В современных условиях государство, любая организация (предприятие) и каждый человек могут стать жертвой киберпреступников. Киберпреступлениями причиняется реальный ущерб, и они могут совершаться в различных сферах, например, финансово-кредитной, промышленности, на различных объектах разных форм собственности (например, критически важный объект информатизации или частное предприятие). Каждая из этих сфер и объектов имеют свои особенности, связанные с обеспечением информационной безопасности, в отдельных случаях требуется индивидуальный подход.

Вопросы кибербезопасности приобретают стратегическое значение как фактор обеспечения национальной безопасности, суверенитета, обороноспособности государства, устойчивого развития экономики и развития различных его сфер [1, с. 756].

Тенденция зарегистрированных киберпреступлений за последние 5 лет такова, что с 2018 по 2021 года фиксировался их рост более чем на 200 процентов, в последующем – в 2021 году зафиксировано снижение числа киберпреступлений, в 2022 году – также, однако уже менее значительное. Анализ статистических данных указывает на волнообразный рост количества киберпреступлений, что связано с применением киберпреступниками новых способов совершения преступлений. Например, в 2020 году рост был обусловлен применением новых способов хищения денежных средств с использованием реквизитов банковских платежных карточек. Однако, несмотря на общее снижение числа киберпреступлений следует отметить, что в настоящее время снижение наблюдается только по сравнению с 2020 годом, снижение количества киберпреступлений до уровня 2019 года за последние годы не произошло. С учетом развития компьютерных сетей, в том числе компьютерной сети Интернет, киберпреступления становятся все более массовым явлением.

К условиям, влияющим на рост киберпреступлений можно, например, отнести устаревшую или неполную защиту компьютерных систем (сетей), определенный уровень специалистов по разработке средств кибератаки, реализация автоматизации проведения таких атак и совершения киберпреступлений. Особенности являются, например, масштабные кибератаки на информационную инфраструктуру, размытый периметр защищаемой инфраструктуры, сложность процессов реагирования, кризис доверия к зарубежным технологиям.

Появление новых информационных технологий обуславливает и то, что в скором времени появятся новые способы совершения киберпреступлений и новые формы их проявлений. Это должно нацелить уполномоченные органы на своевременное предупреждение киберпреступлений, при том, что в ближайшее время данный вид преступления может занять одно из лидирующих мест в структуре преступности.

Совершенствование деятельности по предупреждению киберпреступлений продиктовано необходимостью объединения усилий всех заинтересованных субъектов, начиная от правоохранительных органов и иных государственных органов до учреждений образования, осуществляющих подготовку специалистов в области информационной безопасности, заканчивая банками и частными компаниями.

При этом невысокий уровень их раскрываемости обуславливается эволюционированием киберпреступлений, характеризующихся реализацией новых схем их совершения, трансформацией средств совершения, а также их трансграничным характером, а также особенностями установления лиц их совершивших. В свою очередь, правоохранительные органы и иные уполномоченные субъекты ведут борьбу

преимущественно с последствиями киберпреступлений, при этом прямая борьба осложняется рядом факторов и целесообразнее более активно использовать механизмы их предупреждения.

В комплекс мер предупредительного характера должны входить меры, различной направленности такие как создающие сложности совершения киберпреступлений, повышающие риск при их совершении, так и уменьшающие выгоду от совершения киберпреступления, и по своей сути они должны носить правовой, организационный и технический характер.

Касаясь мер правового характера, необходимо отметить, что на современном этапе реализуется принятие нормативных правовых актов, направленных на противодействие современным угрозам в информационной сфере, наблюдается стремление к совершенствованию подходов в сфере кибербезопасности различными ведомствами, банками и другими учреждениями (организациями).

В свою очередь, возможна проработка вопроса об усилении административной и уголовной ответственности за совершение киберпреступлений (правонарушений), в настоящее время можно констатировать, что в отдельных случаях возможно несоответствие наказания причиненному ущербу.

Актуально дальнейшее развитие правовых механизмов усложнения легализации денежных средств, полученных преступным путем, в том числе в виде криптовалют. При этом надо учитывать, что для осуществления преступной деятельности также необходимо ее финансовое обеспечение как в самом начале, так и процессе ее осуществления (за непродолжительное время значительные суммы денежных средств могут быть переведены с выявленного банковского счета), при этом основные меры принимаются в рамках уголовного дела, что требует распространения таких правовых механизмов на более ранние этапы, когда проводится проверка по материалам о преступлениях или работа по делам оперативного учета.

Целесообразно формирование в обществе, а также в среде киберпреступников, убежденности в способности государства обеспечить национальную безопасность в информационной сфере. Киберпреступник должен понимать высокую степень вероятности привлечения его к уголовной ответственности в случае совершения им преступления.

Касаясь мер организационного характера в предупреждении киберпреступлений, целесообразно отметить проблемные аспекты этой деятельности, к которым можно отнести, например, длительное получение информации от интернет-провайдеров и банков; использование банковских счетов, сим-карт, оформленных на других лиц; использование технологий, противодействующих идентификации лиц в сети Интернет; отсутствие дополнительных мер аутентификации и верификации кредитополучателя при онлайн-кредитовании; выдача онлайн-кредитов на сумму в десятки раз превышающую месячный доход получателя; продолжительный срок формирования кредитной истории и внесение сведений в кредитный регистр (возможность оформить на жертву несколько кредитов).

В свою очередь следует отметить, что, например, ввиду технических особенностей большинства вредоносного программного обеспечения, основным условием совершения преступлений с использованием такого программного обеспечения является именно активные действия жертвы для внедрения его в файловую систему и инициализацию работы. Виктимное поведение пользователей информационных систем, обусловленное цифровой неграмотностью, является ключевым условием совершения ряда киберпреступлений. Работа, осуществляемая заинтересованными субъектами по повышению цифровой грамотности населения, которая заключается в массовом проведении представителями различных органов государственного управления, в том числе и правоохранительными органами, профилактических бесед с различными слоями населения; размещению наглядных материалов в виде листовок, брошюр, социальной рекламы в местах массового нахождения граждан; разъяснение основных мер предосторожности при попытках преступных посягательств в средствах массовой информации (телевидение, интернет-ресурсы и др.). При этом проводимая в настоящее время работа по профилактике киберпреступности в большей

степени направлена на устранение виктимного поведения граждан при совершении преступлений, предусмотренных статьями 209, 212 (мошенничество, хищение путем модификации компьютерной информации) Уголовного кодекса Республики Беларусь. Особо актуальна данная работа в отношении работников, которые в связи со своим должностным положением выполняют работу по обработке информации. Также возникла необходимость формирования определенного уровня цифровой грамотности населения посредством образовательной системы, вопрос цифровой грамотности гражданина выводится на уровень образовательного (воспитательного) процесса еще на стадии детского возраста с целью присвоения несовершеннолетним критического взгляда на действия, совершаемые в компьютерной сети Интернет.

В целом организационные меры предупреждения киберпреступлений в большей степени актуальны для организаций, так как они нередко являются владельцами информационных систем, хранящих те или иные данные, представляющие интерес для злоумышленников, а некомпетентные действия сотрудников нередко приводит к внедрению вредоносного программного обеспечения в указанные информационные системы.

Отдельным элементом в деятельности по предупреждению киберпреступлений является проведение профилактической работы с гражданами, от которых можно ожидать совершение подобных квалифицированных преступлений. Криминогенной склонностью могут обладать молодые люди, обладающие специальными компетенциями, в определенной степени это касается несовершеннолетних, проходящих обучение по направлению информационных технологий, а также студентов учреждений образования по направлениям, связанным с информационными технологиями. Основным профилактическим воздействием выступает разъяснение норм законодательства, регулирующего данную сферу, в частности разъяснение мер уголовного наказания за совершение киберпреступлений и в целом разъяснение перечня деяний, подпадающих под административную ответственность в данной сфере, что обусловлено недостаточным уровнем правовой грамотности населения, приводящий иногда к совершению киберпреступлений ввиду незнания правового запрета на совершения отдельных действий.

Вопрос оказания профилактического воздействия на лиц, ранее судимых за киберпреступления, также представляет интерес и требует приложения усилий не только правоохранительных органов, но и совместной скоординированной работы различных субъектов.

Касаясь мер технического характера, необходимо отметить, что целесообразно смещение акцента и реализация более широкого спектра мер защиты на уровне интернет-провайдеров, операторов сотовой связи и банков, а не на уровне конечного пользователя (например, физическое лицо, организация).

Целесообразна проработка вопроса по совершенствованию и четкой регламентации механизмов взаимодействия между клиентом и банком, между банком отправителя и банком получателя денежных средств, в случае совершения преступления и их хищения. С целью предупреждения киберпреступлений банками и небанковскими кредитно-финансовыми организациями целесообразно предусмотреть обязательное информирование клиентов о каждой проведенной операции по банковским счетам; постоянное совершенствование механизмов по подтверждению платежа и доступа к кабинету системы дистанционного банковского обслуживания; постоянное совершенствование системы антифрода; внедрение программных средств формирования и получения сведений из кредитного регистра; определение каналов связи, объема информации и ответственных лиц по оперативному обмену информацией с уполномоченными правоохранительными органами и др.

В условиях усложнения процесса осуществления, возрастания требований к субъектам различного уровня, решение задач по профилактике киберпреступлений невозможно только путем наращивания сил и средств. Решению этой проблемы может способствовать и внедрение в эту деятельность информационных технологий, такой процесс является современным этапом их эволюции в контексте средств профилактики преступлений. При наблюдаемом в настоящее время повышении значимости сети Интернет во всех сферах

человеческой деятельности, происходит игнорирование ее возможностей в профилактике киберпреступлений. Сегодня почти отсутствуют комплексные информационные ресурсы, специально посвященные предупреждению киберпреступлений, которые могли бы расширить практику профилактической работы правоохранительных и иных государственных органов, организовать обмен информацией с пользователями. Значение такого информационного ресурса невозможно переоценить, его внедрение способствует новому видению существующих и созданию новых способов профилактики киберпреступлений.

При этом одного совершенствования программно-технического обеспечения в сфере обеспечения кибербезопасности недостаточно, эффективно бороться со всеми проявлениями киберпреступности возможно при возникновении условий, при которых технологии в сфере кибербезопасности становятся эффективными только в том случае, если в обществе осознают необходимость процессов противодействия данному явлению и должным образом стремятся к их совершенствованию [2, с. 102].

Таким образом, в настоящее время имеются резервы повышения эффективности деятельности по предупреждению киберпреступлений, которая должна осуществляться не как средство, обеспечивающее привлечение к уголовной ответственности, при этом должно быть обеспечено использование всего комплекса сил, средств и методов и акцент смещен на доприступные формы поведения лиц, при этом реализованы меры как правового, так и организационного и технического характера.

Современное состояние деятельности по предупреждению киберпреступлений имеет ряд аспектов для совершенствования, касающихся вопросов взаимодействия различных субъектов к которым относятся: противоречие между характером решаемой комплексной задачи и структурной разобщенностью; невозможность эффективного решения комплексной задачи, только собственными силами и средствами.

Литература

1. Аминов, И.И. Предупреждение киберпреступлений в финансовой сфере / И.И. Аминов // Научно-практический электронный журнал Аллея Науки. – 2018. – Т. 5, № 6(22). – С. 754–758.
2. Кобец, П.Н. Правовые основы предупреждения киберпреступлений: отечественный и зарубежный опыт / П.Н. Кобец // Научный вестник Омской академии МВД России. – 2022. – Т. 28, № 2(85). – С. 101–105.

ОПЕРАТИВНО-РОЗЫСКНОЕ ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ, СВЯЗАННЫМ С ПРОТЕСТНОЙ АКТИВНОСТЬЮ ГРАЖДАН (НА ПРИМЕРЕ ИСПОЛЬЗОВАНИЯ ВОЗМОЖНОСТЕЙ ГЛОБАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ ИНТЕРНЕТ)

А.Н. ТУКАЛО

*Учреждение образования «Академия Министерства внутренних дел Республики Беларусь»,
г. Минск, Республика Беларусь*

Введение

«Протестная активность граждан» – термин, который основательно вошел в оборот правоохранительных органов Республики Беларусь с 2020 года, когда была предпринята попытка проведения «цветной революции» в нашей стране. «Цветными революциями» чаще всего называют серию массовых уличных протестов населения, конечной целью которых является смена политической власти в государстве. За последние двадцать лет в мире произошло больше революций, чем за весь XX век.

Методы осуществления «цветных революций» продолжают постоянно модернизироваться и совершаться. До настоящего времени проходят протесты в Республике Молдова, Французской Республике, Государстве Израиль, в том числе продолжаются попытки осуществить «цветную революция» в Республике Беларусь (на чем неоднократно акцентировал внимание Глава государства в своем ежегодном послании белорусскому народу и Национальному собранию 31 марта 2023 года).

Очевидно, что попытки дестабилизировать ситуацию на территории Союзного государства России и Беларуси будут продолжаться и в дальнейшем, что требует принятия действенных мер противодействия (информационно-идеологических, правовых, оперативно-розыскных и т.д.).

В настоящее время, значительная часть преступлений, связанных с протестной активностью граждан (около 80 %), совершаются в глобальной компьютерной сети Интернет [1, с. 4.]. К ним относятся преступления, предусмотренные ст. ст. 130, 130-1, 188, 203-1, 341, 361-1, 361-2, 361-3, 361-4, 361-5, 342, 364, 366, 367, 368, 369, 369-1, 369-3, 370, 391 УК Республики Беларусь [2] и многие другие. Большинство указанных преступлений совершаются в отношении государственных служащих, сотрудников правоохранительных органов и иных представителей власти с использованием мессенджеров «Telegram», «Viber» и различных популярных социальных сетей таких как: «ВКонтакте», «Twitter», «Instagram», «Одноклассники», реже «Facebook». Как показывает правоохранительная практика, наиболее часто данная категория преступлений, на сегодняшний день совершается посредством мессенджера «Telegram». В настоящее время кроссплатформенная система мгновенного обмена сообщениями «Telegram» пользуется огромной популярностью во всем мире, особенно в молодежной среде, считается одной из наиболее защищенной и одновременно приватной и насчитывает более полумиллиарда пользователей. Требуется унификация оперативно-розыскного законодательства России и Беларуси [3] с целью повышения эффективности противодействия преступлениям, связанным с протестной активностью граждан и выявления лиц их совершающих.

Так на сегодняшний день в Республики Беларусь функционируют различные деструктивные Telegram-каналы и чаты («Вурол», «NEXTA», «РАЛЬНАЯ БЕЛАРУСЬ» и тому подобные). На указанных ресурсах на постоянной основе публикуется различного рода информация, направленная на дискредитацию деятельности государственных служащих и сотрудников правоохранительных органов. Периодически размещаются призывы к совершению противоправных действий в отношении таких лиц. Очевидно, что вышеуказанная деятельность в соответствии со ст. 1 Закона Республики Беларусь от 14 мая 2021 г. № 104-3 «О противодействии экстремизму» является экстремистской [4].

С целью сокрытия своих преступных деяний, пользователи мессенджера «Telegram» и вышеуказанных социальных сетей зачастую максимально скрывают информацию об идентификаторах, которые возможно скрыть с помощью настроек конфиденциальности (приватности) либо же не скрывают данную информацию, а умышленно указывают ненастоящие (вымышленные анкетные сведения). Правоохранительными органами Беларуси выработан действенный механизм по деанонимизации таких пользователей и документирования их противоправной деятельности.

На первоначальном этапе, с целью раскрытия и документирования преступной деятельности пользователей сети Интернет, необходимо получить как можно больше информации об установочных данных таких лиц и используемых ими аккаунтах для последующего их анализа. В социальных сетях («ВКонтакте», «Instagram», «Одноклассники», «Twitter», «Facebook») основным неизменным идентификатором является персональная, существующая в единственном экземпляре ссылка на страницу той или иной социальной сети либо же уникальный ID номер персональной страницы профиля, что не составляет трудностей в идентификации пользователя, то наиболее сложноустроенным по своей структуре является мессенджер «Telegram».

Существуют много аналоговых версии мессенджера «Telegram», позволяющие сразу просмотреть ID того или иного пользователя при открытии информации о нем. Наиболее популярными и простыми в использовании являются «BGRAM» и «Kotatogram». Также, с целью установления ID можно использовать различные специальные Telegram-боты, позволяющие просмотреть ID и иную информацию о том или ином пользователе: CheckID, AIDbot, IDBot, Userinfobot и другие (как правило они отображают сведения об ID, User Name, Имени пользователя). Когда установлен ID аккаунта, в дальнейшем проводятся комплекс дополнительных мер по деанонимизации (вычислению иных личных данных, например, абонентский номер телефона, привязанный к аккаунту) того или иного пользователя, что в итоге позволяет установить конкретное физическое лицо, которое использует проверяемый аккаунт.

Зачастую, имея ID пользователя либо ID страницы (электронный адрес) на первоначальном этапе оперативному сотруднику необходимо определить по каким идентификаторам будет осуществляться поиск вышеуказанной информации и какие Telegram-боты, позволяющие получить информацию, которая может способствовать отождествлению того или иного пользователя (конкретного человека, его активности в сети Интернет) и иные сведения, он будет использовать. Рассмотрим отдельные из них.

1. Quick OSINT бот. Данный Telegram-бот позволяет искать информацию по различным идентификаторам (абонентский номер оператора сотовой связи, электронный адрес почты, фотоизображение, IMEI телефона, электронный адрес страницы профиля социальных сетей, IP-адрес, ID-Telegram и другие).

2. Eye Of God («Глаз бога»). Аналогичный Quick OSINT боту наиболее популярный на сегодняшний день. Поиск информации можно осуществить по таким же идентификаторам, как и в Quick OSINT бот.

3. Usersbox-бот (созданный на базе OSINT). Отличительной особенностью данного бота от вышеуказанных является то, что он в отдельных случаях позволяет отследить историю изменения имени или никнейма.

4. VkUserInfo бот. Данный бот позволяет осуществлять поиск информации только лишь по ссылке (электронному адресу) страницы «ВКонтакте». После чего имеется возможность осуществить поиск по двум дополнительным разделам: «вузы» и «города». Суть заключается в том, что бот в автоматическом режиме анализирует, аккумулирует и в итоге выдает информацию в виде небольшого отчета о друзьях искомого пользователя (а именно в каких городах они проживают и в каких учебных заведениях состоят).

5. Eye of Beholder бот. Уникальный в своем роде Telegram-бот, не имеющий на сегодняшний день подобных аналогов. Позволяет получить информацию, чем интересовался тот или иной пользователь в Интернете с указанием примерного периода времени, получить историю изменения имени (с указанием конкретной даты, когда оно было изменено), историю

осуществляемых пользователем публикаций в сети Интернет, группы в которых состоит пользователь и другие (поиск осуществляется по абонентскому номеру либо ID-Telegram).

На последующем этапе проводится комплекс оперативно-розыскных мероприятий с целью документирования противоправной деятельности уже установленного пользователя.

Таким образом, используя в совокупности вышеуказанные способы поиска оперативной информации, можно получить множество сведений, позволяющих в дальнейшем идентифицировать конкретного пользователя (человека). Полученные сведения необходимо проверить или же сопоставить со сведениями, имеющимся в различных базах данных в правоохранительных органах, например, «АИС Паспорт», «МИАС» и др. (подробнее технологии OSINT рассмотрены в ряде работ автора [5, 6]). Проанализировав полученную в совокупности информацию, можно установить конкретного пользователя мессенджера «Telegram» либо же пользователя искомой персональной страницы профиля социальной сети и используемые им идентификаторы.

Заключение

Таким образом, используя вышеуказанные сервисы, можно находить точные либо возможные взаимосвязи об искомом объекте (в нашем случае это лица, которые совершают преступление связанные с протестной активностью граждан в сети Интернет) либо возможные взаимосвязи о искомом объекте, обнаруживать совпадения между ними, структурировать полученные данные в один поисковый результат по аналогии с поисковыми системами, анализировать полученные данные.

Литература

1. Теория и практика информационного противодействия экстремистской и террористической деятельности: монография / Судиев И.Ю., Смирнова А.А., Кундетов А.И., Федотов В.П.; М-во внутр. дел. Рос. Федерации, Всесоюз.Науч.-исслед. Ин-т.– Москва; Волгоград: Полиграф-Книга, 2014. – 240 с.

2. Уголовный кодекс Республики Беларусь с изм. и доп., от 9 июля 1999г. № 275-З, принятый Палатой представителей 2 июня 1999 года, одобренный Советом Республики 24 июня 1999 года // Консультант Плюс: Беларусь. Технология 3000 [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

3. Тукало, А.Н. Оперативно-розыскное законодательство Союзного государства России и Беларуси: перспективы становления и развития: учебное пособие / А.Н. Тукало [и др.]: учреждение образования «Омская акад. М-ва внутр. дел России». – Омск: Омская акад. МВД России, 2020. – 104 с.

4. О противодействии экстремизму: Закон Республики Беларусь от 14 мая 2021 г. № 104-З // Консультант Плюс: Беларусь. Технология 3000 [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

5. Тукало, А. Н. Общедоступные вспомогательные сервисы установления персональных данных и иной значимой информации в деятельности сотрудников правоохранительных органов / А. Н. Тукало // Цифровизация деятельности судов: текущие и перспективные задачи: междунар. науч.–практ. семинар., (Ташкент, 28 апреля 2022 г.): сб. науч.-практ. семинара // Ташкентский государственный юридический университет. – Ташкент. – С. 55–58.

6. Тукало, А.Н. Особенности проведения оперативно-розыскного мероприятия «оперативный опрос» в сети Интернет // Я.А. Высоцкий, А.Н. Тукало // Проблемы оперативно-розыскного обеспечения уголовного процесса: материалы Респ. науч.-практ. конф., Минск, 7 июня 2019 г.: тез. докл. / учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь» – Минск: Академия МВД, 2019. – С. 105–107.

ЗАСЕДАНИЕ № 4

КРИПТОГРАФИЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.421.6: 519.23

О ПРИМЕНЕНИИ ПРОГРАММНОГО КОМПЛЕКСА «ЭАДП» ДЛЯ СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ

В.Ю. ПАЛУХА, Ю.С. ХАРИН

*НИИ прикладных проблем математики и информатики,
Белорусский государственный университет
г. Минск, 220030, Республика Беларусь*

Введение

Одним из важнейших элементов систем криптографической защиты информации (СКЗИ) являются генераторы случайных и псевдослучайных последовательностей. Стойкость СКЗИ зависит от того, насколько близка генерируемая последовательность по своим свойствам к равномерно распределенной случайной последовательности (РРСП) [1], которая на практике называется «чисто случайной» последовательностью.

Для проверки качества криптографических генераторов используются статистические тесты, в которых проверяется гипотеза $H_* = \{\{x_i\} \text{ является РРСП}\}$ о том, что наблюдаемая последовательность $\{x_i\}$ является равномерно распределенной случайной последовательностью. В НИИ ПМИ разработан программный комплекс «Энтропийный анализ дискретных последовательностей» (ПК «ЭАДП») [2], в котором в качестве тестовых статистик используются статистические оценки функционалов энтропии Шеннона, Реньи и Тсаллиса (с параметром $r = 2$).

Оценки энтропии. Пусть на вероятностном пространстве (Ω, F, P) определена случайная величина x из алфавита мощности $N = 2^s$ с дискретным распределением вероятностей $p = \{p_k\}, p_k = P\{x = \omega_k\}, p_k \geq 0, \sum_{k=1}^N p_k = 1, k = 1, \dots, N$. В таблице 1 приведены формулы функционалов энтропии, используемых в ПК «ЭАДП».

Таблица 1. – Функционалы энтропии

Энтропия Шеннона	$H(p) = -\sum_{i=1}^N p_i \ln p_i$
Энтропия Реньи ($r = 2$)	$H_2(p) = -\ln \left(\sum_{i=1}^N p_i^2 \right)$
Энтропия Тсаллиса ($r = 2$)	$S_2(p) = 1 - \sum_{i=1}^N p_i^2$

Пусть имеется случайная последовательность $\{x_t : t = 1, \dots, n\}$ объема n из распределения вероятностей $\{p_k\}$, по которой будет оцениваться энтропия. Частотные оценки вероятностей имеют вид

$$\hat{p}_k = \frac{v_k}{n}, \quad v_k = \sum_{t=1}^n I\{x_t = \omega_k\} \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}, \quad I\{x_t = \omega_k\} = \begin{cases} 1, & x_t = \omega_k; \\ 0, & x_t \neq \omega_k. \end{cases} \quad (1)$$

Рассмотрим асимптотику совместного увеличения объема выборки и сложности задачи:

$$n, N \rightarrow \infty, n/N \rightarrow \lambda, 0 < \lambda < \infty. \quad (2)$$

В асимптотике (2) для распределения вероятностей статистик $\{v_k\}$ справедлива аппроксимация законом Пуассона $\Pi(\lambda_k)$ с параметром $\lambda_k = np_k$. При истинной гипотезе H_* все элементарные вероятности равны: $p_k = 1/N$, $k = 1, \dots, N$, поэтому все частоты $\{v_k\}$ имеют одинаковый параметр распределения Пуассона $\lambda = n/N$.

Оценка энтропии Шеннона на основе частотных статистик (1) имеет вид:

$$\hat{H} = \hat{H}(n, N) = -\sum_{k=1}^N \hat{p}_k \ln \hat{p}_k = -\sum_{k=1}^N \frac{v_k}{n} \ln \frac{v_k}{n} = \ln n - \frac{1}{n} \sum_{k=1}^N v_k \ln v_k. \quad (3)$$

Теорема 1 [3]. В асимптотике (2) статистика (3) при гипотезе H_* имеет асимптотически нормальное распределение с параметрами

$$\mu_H = \ln n - e^{-\lambda} \sum_{k=1}^{+\infty} \frac{\ln(k+1)\lambda^k}{k!}, \quad (4)$$

$$\sigma_H^2 = \frac{e^{-\lambda}}{n} \sum_{k=1}^{+\infty} \frac{(k+1)\lambda^k}{k!} \ln^2(k+1) - \frac{e^{-2\lambda}}{N} \left(\sum_{k=1}^{+\infty} \frac{\ln(k+1)\lambda^k}{k!} \right)^2 - \frac{e^{-2\lambda}}{n} \left(\sum_{k=1}^{+\infty} \ln(k+1) \frac{\lambda^k}{k!} (k+1-\lambda) \right)^2. \quad (5)$$

Как следует из теоремы 1, в асимптотике (2) оценка (3) является смещенной, и с уменьшением λ смещение растет. Для функционалов энтропии Реньи и Тсаллиса можно построить несмещенную оценку в асимптотике (2), в том числе и при $\lambda < 1$. Для построения несмещенной оценки воспользуемся факториальной степенью $x^2 = x(x-1)$.

Статистические оценки энтропии Реньи и Тсаллиса, построенные с использованием факториальной степени, имеют вид

$$\hat{H}_2(n, N) = -\ln \left(\sum_{k=1}^N \hat{p}_k^2 \right) = 2 \ln n - \ln \sum_{k=1}^N v_k^2, \quad (6)$$

$$\hat{S}_2(n, N) = 1 - \sum_{k=1}^N \hat{p}_k^2 = 1 - \frac{1}{n^2} \sum_{k=1}^N v_k^2. \quad (7)$$

Теорема 2 [3]. В асимптотике (2) статистика (6) является состоятельной оценкой энтропии Реньи и при истинной гипотезе H_* имеет асимптотически нормальное распределение с параметрами:

$$\mu_{H,r} = \ln N, \quad \sigma_{H,2}^2 = \frac{2}{n\lambda}. \quad (8)$$

Теорема 3 [3]. В асимптотике (2) статистика (7) является состоятельной асимптотически несмещенной оценкой энтропии Тсаллиса и при истинной гипотезе H_* имеет асимптотически нормальное распределение с параметрами:

$$\mu_{S,2} = 1 - \frac{1}{N}, \quad \sigma_{S,2}^2 = \frac{2}{Nn^2}. \quad (9)$$

Решающее правило. Пусть $\alpha \in (0, 1)$ – заданный уровень значимости, h – статистическая оценка энтропии Шеннона, Реньи или Тсаллиса, μ_h и σ_h^2 – соответственно асимптотические математическое ожидание и дисперсия этих оценок при истинной гипотезе H_* . Вычислим для наблюдаемой последовательности статистику h . Решающее правило, основанное на статистике h , имеет вид [3]:

$$\text{принимается} \begin{cases} H_*, & \text{если } t_- < h < t_+; \\ \overline{H}_*, & \text{в противном случае,} \end{cases} \quad t_{\pm} = \mu_h \pm \sigma_h \Phi^{-1} \left(1 - \frac{\alpha}{2} \right). \quad (10)$$

где $\Phi(\cdot)$ – функция распределения стандартного нормального закона.

Вычислим нормированную статистику

$$\tilde{h} = \frac{h - \mu_h}{\sigma_h}. \quad (11)$$

Она в асимптотике (1) и при истинной гипотезе H_* имеет стандартное нормальное распределение: $\tilde{h} \sim \mathcal{N}(0, 1)$. Следовательно, двустороннее p -значение для нее равно

$$p\text{-value} = 2 \left(1 - \Phi \left(\left| \tilde{h} \right| \right) \right). \quad (12)$$

Пусть наблюдается двоичная последовательность $\{y_{\tau}\}$, $\tau = 1, \dots, T$. Из непересекающихся подряд идущих фрагментов длины s (s -грамм) $X^{(t)} = (X_j^{(t)}) = (y_{(t-1)s+1}, \dots, y_{ts}) \in \{0, 1\}^s$, $t = 1, \dots, n = \lfloor T/s \rfloor$, сформируем новую последовательность $\{x_t\}$ из алфавита мощности $N = 2^s$ по правилу $x_t = \sum_{j=1}^s 2^{j-1} X_j^{(t)} + 1$. На основе критерия (10) вычислим последовательность нормированных отклонений оценки энтропии от математического ожидания в зависимости от s , которую назовем энтропийным профилем:

$$\chi(s) = \frac{\hat{h}(s) - \mu_h(s)}{\sigma_h(s) \Phi^{-1}(1 - \alpha/2)} = \frac{\tilde{h}(s)}{\Phi^{-1}(1 - \alpha/2)}, \quad s = s_-, \dots, s_+. \quad (13)$$

Аналогично строятся последовательности p -значений (12).

Тестирование с помощью профиля позволяет выносить решение о принятии или отклонении гипотезы H_* на основе решающего правила (10) по совокупности значений $\chi(s)$

для различных s ; такое решение видится более аргументированным, чем при принятии его по результатам применения теста (15) для отдельного значения s . Показана слабая зависимость оценок энтропии по соседним длинам фрагментов [4], тем самым получено обоснование использования энтропийных профилей.

Программный комплекс «ЭАДП». Разработанный в НИИ ППМИ программный комплекс «ЭАДП» реализует критерий (10). В начале работы необходимо выбрать файл с последовательностью, порядок Big Endian или Little Endian, диапазон s и функционалы энтропии. Вычисляемые значения добавляются на экран в режиме реального времени. Имеется возможность изменять уровень значимости α без пересчета оценок энтропии и переключаться на различные режимы отображения: непосредственно оценки энтропии h , нормированные значения (13), p -значения (12). Помимо вывода самих значений в консоль, программа отображает графики зависимостей этих величин от длины фрагмента s . Главное окно программного комплекса с результатами работы представлено на рисунке 1.

Протоколы тестирования с помощью ПК «ЭАДП». Работа ПК «ЭАДП» продемонстрирована путем анализа последовательностей, полученных генераторами случайных и псевдослучайных чисел.

На рисунке 1 отображен энтропийный профиль Реньи последовательности speedtest-500MB.bin физического генератора [5]. Длина последовательности $T = 125 \cdot 2^{25}$. Длина фрагмента $s \in [1, 35]$. Уровень значимости $\alpha = 0,05$. Как видно из рисунка 1, оценки энтропии попадают в интервал допустимых значений при всех значениях s , кроме $s = 26$. Для рассматриваемого генератора гипотеза H_* принимается.

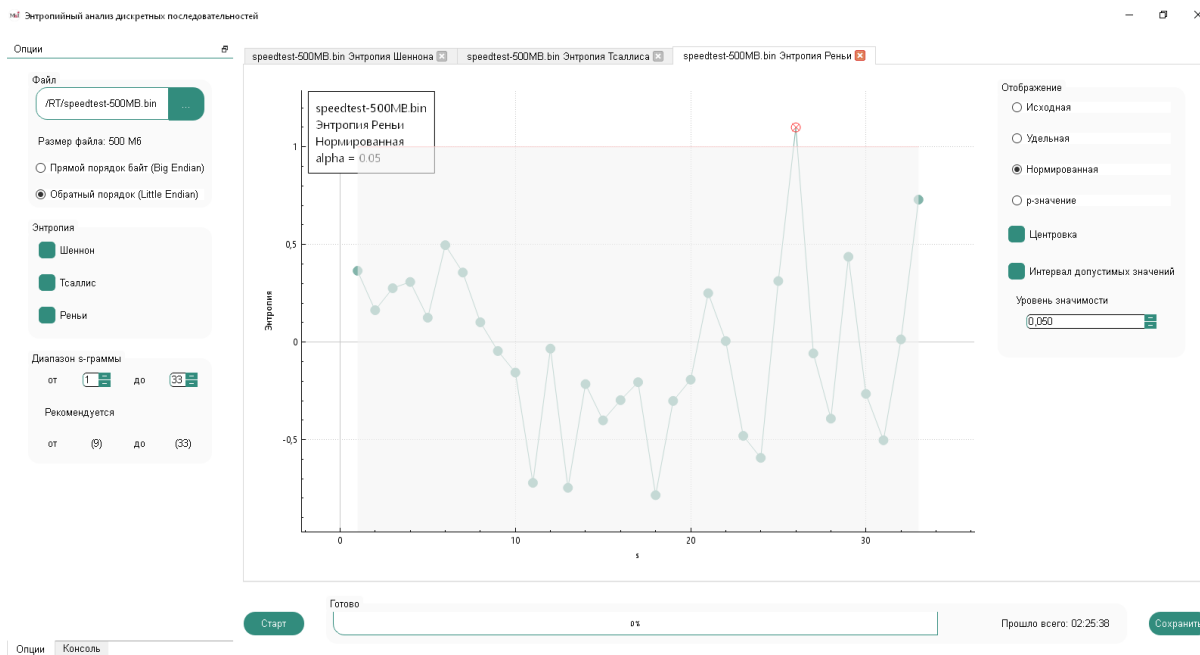


Рисунок 1. – Программный комплекс «ЭАДП». Нормированная энтропия Реньи последовательности speedtest-500MB.bin физического генератора

На рисунке 2 приведен протокол тестирования последовательности алгоритма шифрования VeIT [6] в режиме счетчика с нулевыми ключом и синхрпосылкой. Длина последовательности $T = 2^{30}$. Длина фрагмента $s \in [1, 32]$. Уровень значимости $\alpha = 0,05$. Отображены p -значения критерия на основе оценок энтропии Тсаллиса. Как видно из рисунка 2, оценки энтропии попадают в интервал допустимых значений при всех значениях s , кроме $s = 1$ и $s = 3$. Для рассматриваемого генератора гипотеза H_* принимается.

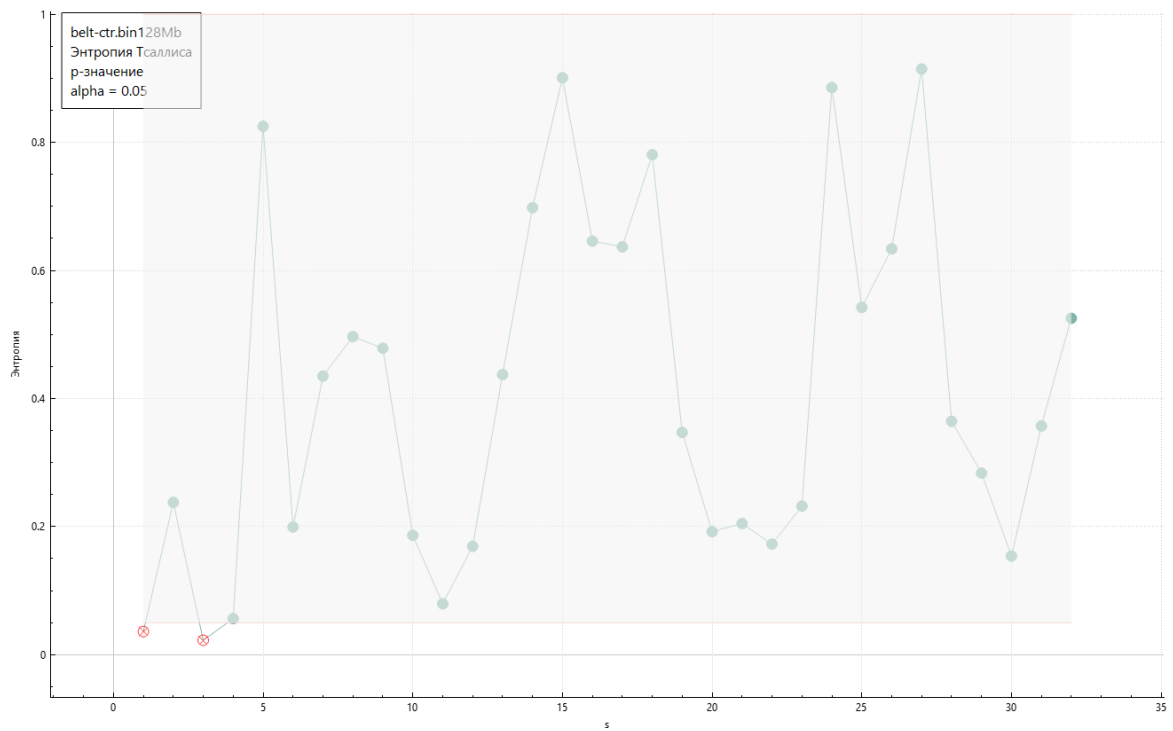


Рисунок 2. – p -значение теста на основе энтропии Тсаллиса последовательности BeIT в режиме счетчика

На рисунке 3 приведен протокол тестирования последовательности самосжимающего генератора [1] на основе регистра сдвига с линейной обратной связью с характеристическим многочленом $x^{10} + x^3 + 1$. Длина последовательности $T = 25 \cdot 2^{25}$. Длина фрагмента $s \in [1, 25]$. Уровень значимости $\alpha = 0,05$. Отображены оценки энтропии Шеннона. Как видно из рисунка 3, начиная с $s = 7$ оценки энтропии не попадают в интервал допустимых значений. Кроме того, наблюдается закономерность в значениях оценок. Для рассматриваемого генератора гипотеза H_* отклоняется.

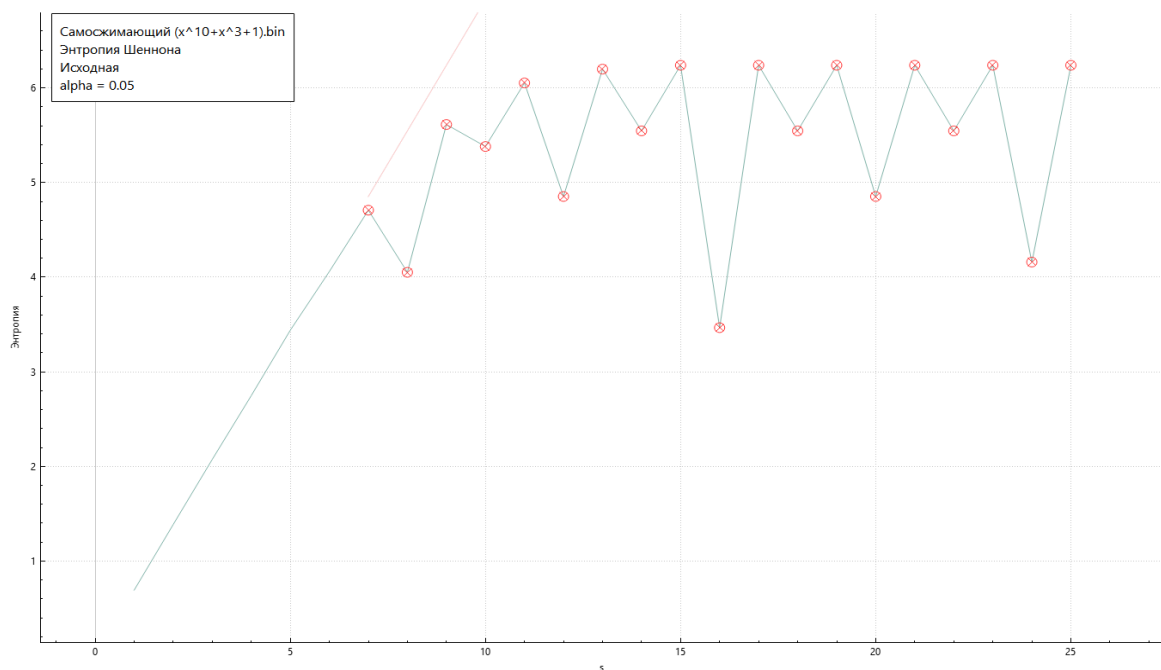


Рисунок 3. – Энтропия Шеннона последовательности самосжимающего генератора

Литература

1. Криптология / Ю.С. Харин [и др.]. – Минск: БГУ, 2013. – 512 с.
2. Программный комплекс «Энтропийный анализ дискретных последовательностей» [Электронный ресурс]. – Режим доступа: http://www.product.bsu.by/katalog/informacionnie-tehnologii/informacionnie-naukoemkie-tehnologii/statistika/programmnoe-sredstvo-entropijnogo-analiza-diskretnih-sluchajnih-posledovatel_nostej/. – Дата доступа: 31.03.2023.
3. 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.
4. Palukha, U.Yu. On statistical testing of random and pseudorandom sequences based on entropy functionals / U.Yu. Palukha, Yu.S. Kharin, A.I. Siarheeu, A.A. Arlou // Computer Data Analysis and Modeling: Stochastics and Data Science. Proceedings of the XIII International Conference, Minsk, September 6–10, 2022 / BSU; eds.: Yu. Kharin [et al.]. – Minsk: BSU, 2022. – P. 148–162.
5. speedtest-500MB.bin [Electronic resource] // Humboldt Berlin University, Faculty of Mathematics and Natural Sciences, Department of Physics. – Mode of access: <http://qrng.physik.hu-berlin.de/files/speedtest-500MB.bin>. – Date of access: 31.03.2022.
6. Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности = Інфармацыйныя тэхналогіі і бяспека. Алгарытмы шыфравання і кантролю цэласнасці: СТБ 34.101.31-2020. – Взамен СТБ 34.101.31-2011; введ. 01.10.20. – Минск: Белорус. гос. ин-т стандартизации и сертификации, 2020. – 44 с.

О ПРИМЕНИМОСТИ БЛОКЧЕЙН-ТЕХНОЛОГИЙ ДЛЯ ХРАНЕНИЯ И ОБРАБОТКИ ИДЕНТИФИКАЦИОННЫХ ДАННЫХ

С.П. ПАНАСЕНКО

Компания «Актив», г. Москва, Россия

Введение

На текущий момент известно уже несколько реализаций на государственном уровне информационных систем, построенных на основе блокчейн-технологий и предназначенных для управления идентификационными данными граждан. В качестве примеров можно привести системы электронных удостоверений личности, разворачиваемые в Бразилии и Эстонии [1, 2].

Рассмотрим принципы хранения и обработки информации в гипотетической системе управления электронными удостоверениями личности на примере паспортов граждан РФ. Паспортные данные в РФ представляют собой совокупность определенных данных (или их подмножество, поскольку часть данных вносится в паспорт по мере необходимости, а некоторые сведения вносятся по желанию владельца паспорта) для каждого гражданина [3], что проиллюстрировано далее на рисунке 1.

1. Использование традиционных баз данных

Рассмотрим паспортные данные с точки зрения их хранения в информационной системе с использованием традиционных БД. Запись совокупности паспортных данных может иметь структуру, крайне упрощенный вариант которой показан на рисунке 1.

В приведенном примере информация, представляющая собой паспортные данные каждого гражданина, может храниться в БД в виде записи в основной таблице «Гражданин», связанной с записями в других таблицах такой БД.

Поскольку практически все поля записи о паспортных данных гражданина могут меняться с течением времени, для идентификации записи необходимо наличие некоего уникального номера (это может быть справедливо и для других таблиц), для чего в таблице присутствует поле «Идентификационный номер», которое может быть использовано для ссылок на запись таблицы из других таблиц и БД связанных информационных систем. В качестве еще одного примера использования идентификационного номера на рисунке 1 можно привести связь через данное поле в таблице «Брак» (поле «Идентификационный номер супруга», которое ссылается на поле «Идентификационный номер» записи о супруге в основной таблице).

Если предположить, что подобная БД является основой некоторой совокупности государственных информационных систем, то информация из такой таблицы будет активно запрашиваться связанными информационными системами. Выборка данных может осуществляться по значениям или диапазонам значений практически всех полей таблиц: поиск граждан может производиться, например, по ФИО или только фамилии, номеру и дате выдачи паспорта (диапазону номеров/дат), подразделению, выдавшему паспорт, дате и месту рождения и т.д. Для ускорения подобных выборок содержимое БД индексируется по всем полям, по которым предполагается поиск, что увеличивает объем хранимых данных, но также значительно увеличивает быстродействие, обеспечивая практически независимость времени поиска от количества записей.

Поскольку различные потребители такой БД (например, различные ведомства РФ) могут иметь разные права на доступ к различным данным таблиц, приведенная выше таблица может быть по факту представлена рядом таблиц, связанных через идентификационный номер гражданина, каждая из которых содержит подмножество данных с одинаковыми правилами доступа к ним (см. рис. 2, связи не приведены). В качестве альтернативного варианта может быть рассмотрена федеративная БД, части которой поддерживаются различными ведомствами.

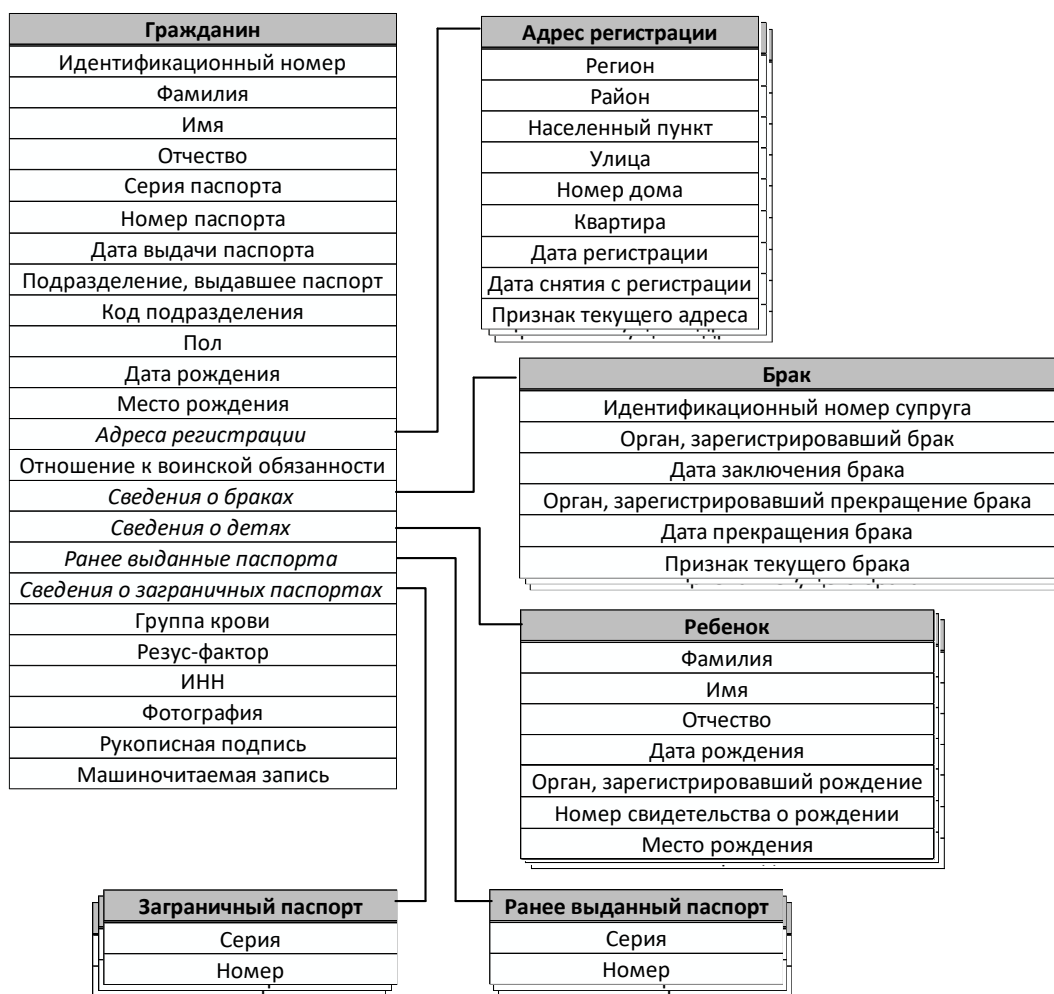


Рисунок 1. – Упрощенная структура записи паспортных данных

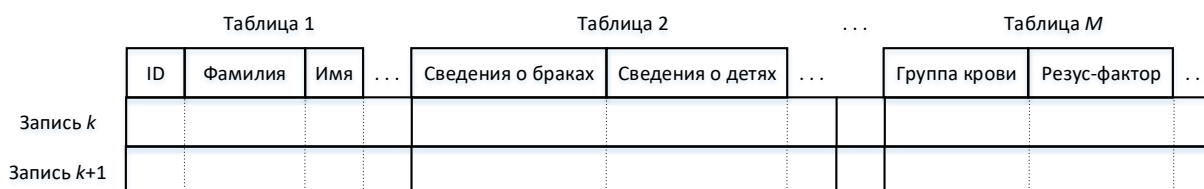


Рисунок 2. – Пример организации таблиц записей о гражданах

Далее под записью будем подразумевать совокупность записей в таблицах 1...M, связанных одним значением идентификатора.

2. Хранение и обработка данных в блокчейне

Если поставить целью использование блокчейн-технологий для хранения и обработки паспортных данных, то эти данные можно хранить и непосредственно в блокчейне. В этом случае каждая транзакция будет добавлять или обновлять некую запись паспортных данных и содержать значения подмножества полей данной записи.

Внутри записи данные могут храниться последовательно в формате, способном хранить некое подмножество значений полей, часть из которых имеет переменный размер. Примером такого формата является формат TLV, явно задающий поле и размер для каждого хранящегося значения. Хранение записей непосредственно в блокчейне, хотя и возможно, не выглядит рациональным, как минимум, по следующим причинам:

- паспортные данные представляют собой конфиденциальную информацию (в РФ паспортные данные относятся к персональным данным, причем совокупность

паспортных данных более 100 000 граждан предусматривает их отнесение к одной из максимально защищаемых категорий персональных данных [4]); при их хранении в блокчейне выглядит крайне сложным организовать надлежащее разграничение доступа к ним;

- разрастание блокчейна, основной причиной которого является невозможность модификации – возможно только добавление данных (см. также далее);
- хранение данных в БД позволяет использовать все их преимущества.

БД позволяют эффективно хранить данные и обеспечивать высокую скорость доступа к ним. «Если ваши требования удовлетворяются современными реляционными базами данных, было бы безумием использовать блокчейн... Почему? Потому что такие продукты, как Oracle и MySQL, имеют за плечами десятилетия разработки. Они были развернуты на миллионах серверов, выполняющих триллионы запросов. Они содержат одни из самых тщательно протестированных, отлаженных и оптимизированных кодов на планете, обрабатывая тысячи транзакций в секунду... А как насчет блокчейнов? Что ж, “наш продукт был одним из первых, вышедших на рынок, и был доступен ровно 5 месяцев, с несколькими тысячами загрузок”» [5].

Использование такого варианта хранения данных является крайне неэффективным с точки зрения поиска требуемых данных. При необходимости выборки при такой «прямой» реализации поиск потребует фактически перебором всех записей от более новых к более старым с проходом по всем блокам цепочки и данным всех транзакций каждого блока (при этом нет гарантии, что требуемый для конкретной выборки набор полей найдется в одной транзакции с данными конкретного гражданина – об этом также см. далее). Для ускорения поиска потребуются введение индексов, которые не выглядит возможным хранить в блокчейне, – для их хранения придется использовать внешнюю по отношению к блокчейну БД.

Таким образом, мы возвращаемся к использованию традиционных БД, поэтому рассмотрим более эффективный вариант совместного применения БД и блокчейна.

3. Фиксация записей с помощью блокчейна

Достаточно часто принято противопоставлять друг другу организацию хранения данных в виде блокчейна и в виде БД. Процитируем работу [6]: «Традиционные базы данных имеют четыре классические операции: вставки, удаления, обновления и выбора... Технология блокчейна эквивалентна базам данных, отказывающимся от возможностей удаления и обновления, оставляя только две манипуляции, вставку и выбор, через структуру цепочки блоков и связанных списков...».

Тем не менее ничто не мешает совместному использованию блокчейна и классической БД, например, следующим образом для рассматриваемого применения:

- классическая БД используется для хранения данных;
- записи БД связываются в цепочку с помощью блокчейна: в блокчейне хранятся хеш-коды записей, размещенных в БД.

Т.е. внешняя БД используется для хранения не индексов, а записей в целом, а блокчейн позволяет зафиксировать эти записи, что проиллюстрировано на рисунке 3.

В отличие от предыдущего варианта хранения данных, в котором БД играла вспомогательную в отношении блокчейна роль, в данном случае именно блокчейн стал вспомогательным по отношению к традиционной БД.

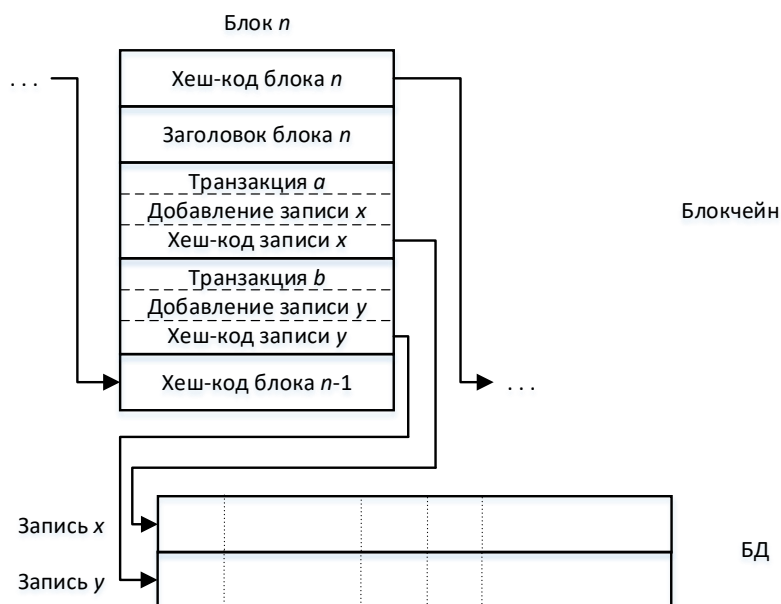


Рисунок 3. – Фиксация записей в блокчейне

При этом относительно легко организовать модификацию данных существующей записи – путем добавления транзакции, содержащей модифицируемое подмножество данных и пересчитанный хеш-код записи (рис. 4).

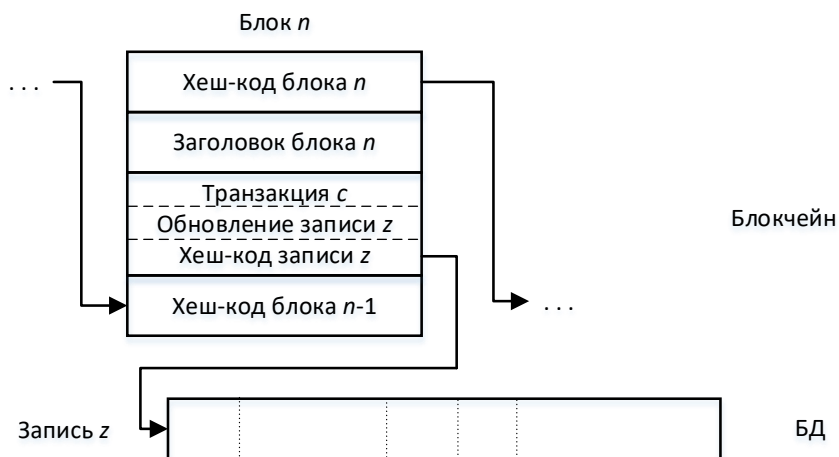


Рисунок 4. – Модификация записи

Возможность модификации данных выглядит однозначно необходимой: во-первых, как упоминалось ранее, значения практически всех полей записи паспортных данных могут изменяться с течением времени; во-вторых, поля любой записи могут заполняться постепенно (за заполнение могут отвечать различные ведомства – см. [3]) – т.е., в случае использования блокчейн-технологий, несколькими транзакциями.

С другой стороны, «append-only» парадигма блокчейн-технологий по отношению к паспортным данным может оказаться единственно верной: выглядит необходимым не только хранить текущие значения всех полей записей, но и их прошлые значения, даты модификации и идентификаторы организаций (должностных лиц), внесших изменения. А поиск и выборка записей могут производиться в случае необходимости и по значениям, актуальным в определенный диапазон прошедших дат.

Однако даже эту парадигму достаточно эффективно можно организовать с помощью традиционных БД вводом дополнительных полей или таблиц, содержащих не только актуальные, но и прошлые значения полей, что было показано на рисунке 1.

Заключение и выводы

В рассмотренной в предыдущем разделе структуре хранения данных все основные функции по хранению данных и организации доступа к ним обеспечиваются применением традиционных БД. Видно, что блокчейн представляет собой лишь ссылочную цепочку хеш-кодов, которая (при необходимости) без потери функционала может быть внесена непосредственно в БД с отказом от блокчейн-структуры, подразумевающей наличие транзакций и их объединение в блоки.

Применение блокчейна в данном случае не может добавить прозрачности, поскольку все данные хранятся вне блокчейна, доступ к ним ограничен в соответствии, в том числе с требованиями по защите персональных данных. Следовательно, единственное, что можно проверить с помощью такого блокчейна – факт наличия в БД записи, совокупность полей которой имеет определенное, записанное в блокчейне, хеш-значение, с привязкой ко времени ее добавления или изменения (но такую проверку может осуществить только обладатель доступа ко всем полям записи). По этой причине можно утверждать, что данная цепочка хеш-значений является избыточной, искусственно привнесенной в систему структурой, вносящей дополнительную сложность в систему; данный блокчейн необходимо поддерживать и хранить – с неясными целями и отсутствием явных преимуществ за счет его применения.

Таким образом, можно сделать вывод о том, что применение блокчейн-технологий для хранения паспортных данных и управления ими не выглядит целесообразным с технической точки зрения, поскольку данные задачи могут быть успешно решены за счет использования традиционных баз данных:

- возможность записи данных в БД различными субъектами системы решается за счет настройки соответствующих прав доступа к различным сущностям;
- вопросы обеспечения неизменности и конфиденциальности данных решаются аналогичным образом в совокупности с применением криптографических методов: хеширования для контроля целостности и, при необходимости, шифрования частей данных с ограниченным доступом;
- доступность данных обеспечивается резервированием компонентов системы, включая создание резервных копий БД с репликацией данных;
- хранение данных, ставших неактуальными, осуществляется вводом дополнительных связанных таблиц, при этом хранение таких данных никак не увеличивает трудоемкость поиска и выборки данных.

Все перечисленные возможности реализуются современными системами управления базами данных. Применение блокчейн-технологий для усиления каких-либо возможностей системы не требуется.

Литература

1. Правительство Бразилии тестирует блокчейн-систему удостоверений личности. // <https://coinmarket.news> – Август 24, 2017.
2. Блокчейн-республика: система «электронного резидентства» в Эстонии создает цифровое общество без границ. // <https://coinmarket.news> – Август 16, 2017.
3. Постановление Правительства Российской Федерации от 8 июля 1997 г. № 828. «Об утверждении Положения о паспорте гражданина Российской Федерации, образца бланка и описания паспорта гражданина Российской Федерации» (в ред. от 15.07.2021 г.).
4. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
5. G. Greenspan. Avoiding the pointless blockchain project. // <https://www.multichain.com> – November 22, 2015.
6. Blockchain White Paper. // <http://www.caict.ac.cn> – December 2018 – China Academy of Information and Communication Technology. Trusted Blockchain Initiatives.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ. ПОДХОДЫ К РЕГУЛИРОВАНИЮ

П.О. БЕГУНЕЦ

*Оперативно-аналитический центр при Президенте Республики Беларусь
г. Минск, 220030, Республика Беларусь*

Цифровая трансформация принесла как множество преимуществ, так и кратное увеличение угроз, в числе которых отдельное место занимают киберугрозы. В быстро развивающемся цифровом ландшафте кибербезопасность стала важнейшим аспектом современного общества, поскольку кибератаки наносят значительный финансовый, репутационный и операционный ущерб. Интеграция искусственного интеллекта и машинного обучения в усилия по обеспечению кибербезопасности представляет собой многообещающее решение этих проблем.

Технологии искусственного интеллекта в системах кибербезопасности предлагают множество преимуществ. Во-первых, они позволяют обнаруживать угрозы и реагировать на них в режиме реального времени, выявляя потенциальные уязвимости и нарушения быстрее, чем традиционные методы. Во-вторых, системы на базе искусственного интеллекта могут адаптироваться и развиваться для противодействия новым и возникающим угрозам, обеспечивая постоянную защиту от динамически меняющихся киберрисков. Наконец, технологии искусственного интеллекта могут автоматизировать повторяющиеся задачи и уменьшить количество человеческих ошибок, позволяя специалистам по кибербезопасности сосредоточиться на более сложных и стратегических аспектах управления безопасностью.

Однако при внедрении искусственного интеллекта в систему обеспечения кибербезопасности имеется вероятность возникновения ряда проблем, в их числе вероятность предвзятых алгоритмов, чрезмерная зависимость от искусственного интеллекта и атаки со стороны противника с использованием технологий искусственного интеллекта. Предвзятые алгоритмы могут непреднамеренно увековечить существующие предубеждения в данных, что приведет к несправедливым или дискриминационным результатам. Чрезмерная зависимость от искусственного интеллекта может привести к самоуспокоенности и снижению бдительности человека, что сделает системы более уязвимыми перед новыми угрозами, которые ИИ может еще не распознать. Кроме того, сами злоумышленники могут использовать системы искусственного интеллекта, запуская состязательные атаки, манипулируя процессом обучения искусственного интеллекта или используя дипфейки, созданные такими технологиями, для обхода мер безопасности. Эти проблемы подчеркивают необходимость сбалансированного подхода к интеграции искусственного интеллекта в систему обеспечения кибербезопасности с постоянным человеческим контролем и регулярными обновлениями для устранения возникающих угроз.

Для устойчивого и безопасного развития систем обеспечения кибербезопасности использующих технологии искусственного интеллекта стоит обратить внимание на принципы искусственного интеллекта, сформулированные Организацией экономического сотрудничества и развития. Данные принципы подчеркивают, что искусственный интеллект должен быть разработан на благо людей и планеты при соблюдении ценностей и справедливости, ориентированных на человека. Кроме того, системы искусственного интеллекта должны быть прозрачными, безопасными, надежными и подотчетными, чтобы обеспечить надежность и защитить конфиденциальность. Основным инструментом для регулирования исследования, развития и внедрения является всеобъемлющая правовая и этическая основа. Правительства, лидеры отрасли и академические учреждения должны сотрудничать для разработки политик и правил, обеспечивающих ответственное развитие и использование технологий искусственного интеллекта. Эти правила должны решать такие

вопросы, как конфиденциальность данных, предвзятость алгоритмов и потенциальное неправомерное использование искусственного интеллекта в злонамеренных целях.

В заключение следует отметить, что растущая интеграция технологий искусственного интеллекта в системы обеспечения кибербезопасности значительно расширила возможности организаций по защите своих цифровых активов и инфраструктуры. Однако быстрое развитие технологий искусственного интеллекта также сопряжено с потенциальными рисками и проблемами, которые необходимо решать с помощью эффективного регулирования и управления. Крайне важно, чтобы заинтересованные стороны, в том числе правительства, промышленность и академические круги, сотрудничали и вносили свой вклад в создание надежной нормативно-правовой базы, обеспечивающей ответственное и этичное использование искусственного интеллекта в системе обеспечения кибербезопасности, одновременно способствуя инновациям и сохраняя конкурентное преимущество в глобальном цифровом ландшафте.

Литература

1. Принципы искусственного интеллекта. Организация экономического сотрудничества и развития – www.oecd.ai/en/dashboards/ai-principles

2. Правовое регулирование искусственного интеллекта: регулирование в России, иностранные исследования и практика. И.А. Филипова

Авторы

Бегунец П.О., сотрудник Оперативно-аналитического центра при Президенте Республики Беларусь.

Адрес для корреспонденции

220030, Республика Беларусь,

г. Минск, ул. Кирова, 49, Оперативно-аналитический центр при Президенте Республики Беларусь
+375 17 309 23 31

Email: bpo@oac.gov.by

МЕТОД ФОРМИРОВАНИЯ ОБЩЕГО СЕКРЕТА С ПОМОЩЬЮ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

М.Л. РАДЮКЕВИЧ

*Научно-производственное республиканское унитарное предприятие
«Научно-исследовательский институт технической защиты информации»,
г. Минск, Республика Беларусь*

Введение

В настоящее время широкую популярность приобретают разработки криптографических алгоритмов, устойчивых к атакам квантовых компьютеров. Данные исследования получили название постквантовая криптография. Квантовые компьютеры могут решать определенные задачи, такие как факторизация больших чисел и дискретный логарифм, гораздо быстрее, чем классические компьютеры. Это означает, что многие существующие криптоалгоритмы, которые основаны на сложности этих задач, могут быть легко взломаны. Постквантовая криптография является важной областью развития криптографии, так как она позволяет сохранить безопасность информации в будущем, когда квантовые компьютеры станут более распространенными. Одним из направлений развития являются методы, использующие синхронизированные искусственные нейронные сети (СИНС). Данные методы основаны на различии между однонаправленной и двунаправленной синхронизацией нейронных сетей, а не на теории чисел, что делает данные методы перспективными. Основная привлекательность данной технологии в случае ее использования в криптографических приложениях состоит в простоте реализации и исключении применения классических однонаправленных математических функций. В данной статье рассмотрен один из методов формирования общего секретного числа с помощью СИНС и выполнена оценка его криптостойкости и быстродействия по отношению к классической технологии (Synchronization of Neural Networks).

Оценка криптостойкости и быстродействия метода формирования общего секретного числа с помощью СИНС

Процесс синхронизации нейронных сетей наиболее часто рассматривается в терминах взаимного обучения искусственных нейронных сетей. Суть классической технологии СИНС описана в [1–4]. На основе данной технологии разработан более криптостойкий и быстродействующий метод (далее – комбинированный метод с секретной модификацией) [5], состоящий из следующих этапов:

1. Задание входных параметров СИНС: n – количество входов каждого персептрона; K – количество персептронов; $\pm L$ – интервал возможных значений весовых коэффициентов персептронов; r – количество строк для функции свертки; d_{yc} – количество тактов синхронизации; V – количество инвертируемых бит;

2. Синхронизация искусственных нейронных сетей (ИНС) [6] абонентов A и B до достижения d_{yc} . Данный шаг повторяется r раз. На выходе данного шага получаем бинарные последовательности (БП) $S_r^A(d_{yc})$ и $S_r^B(d_{yc})$.

3. Выполнение функции свертки (сложение по модулю 2) r БП, полученных на шаге 2;

4. Внесение некоторых изменений в бинарную последовательность $S_r^A(d_{yc})$ абонентом A и в $S_r^B(d_{yc})$ абонентом B , инвертировав случайным образом независимо друг от друга V бит.

5. Устранение несовпадений [7] путем вычисления «четности» каждой пары битов $C_i^A = a_j \oplus a_{j+1}$, $C_i^B = b_j \oplus b_{j+1}$, где i -номер пары, a_j, b_j – j -тый бит A и B соответственно. Абоненты A и B сообщают четности пар друг другу по открытому каналу связи и каждый сравнивает четности соответствующих пар C_i^A с C_i^B . Пары битов, имеющие одинаковую

четность, остаются в БП, а пары с несовпадающими четностями удаляются. В оставшихся парах имеет место либо 0 несовпадающих битов, т.е. $a_j = b_j$ и $a_{j+1} = b_{j+1}$, либо 2, т.е. $a_j \neq b_j$ и $a_{j+1} \neq b_{j+1}$. Так как оглашение четности пары позволяет выразить один неизвестный бит через четность и другой бит $a_j = C_i^A - b_j$ и $a_{j+1} = C_i^B - b_{j+1}$, то для сохранения секретности из каждой пары удаляется по договоренности один бит. Отобранные таким образом биты объединяются в промежуточные БП, которые содержат меньшую долю несовпадающих битов. Повторяя описанную процедуру еще несколько раз, получаем полностью совпадающие бинарные последовательности.

Аналитический анализ процессов, протекающих в СИНС, представляет очень сложную задачу, поэтому используется метод статистического моделирования. Для проведения такого моделирования разработана программная модель, позволяющая получить статистические данные [8].

Исследование криптостойкости данной технологии заключается в следующем. Криптоаналитик, владея полной информацией о параметрах ИНС абонентов А и В и прослушивая канал связи между ними, пытается установить сформированное общее секретное число. Наиболее очевидным является полный перебор значений весовых коэффициентов (ВК). Объем такого перебора при выбранных параметрах ИНС ($L = 8, K = 3, n = 1000$) составляет $2,2 \times 10^{3691}$.

Более эффективными атаками на технологию СИНС являются атаки, при которых криптоаналитик имеет ИНС с такими же параметрами как у абонентов А и В и пытается синхронизировать свою ИНС с ИНС А и В. Рассматривались простая атака и геометрическая. Геометрическая атака является более эффективной и при исследованиях безопасности формирования общего секрета подразумевается ее использование [4].

Также применима атака отложенным перебором [9]. Суть которой заключается в том, что криптоаналитик записывает процесс синхронизации ИНС А и В и, имея множество начальных значений векторов ВК, пытается с помощью геометрической атаки подобрать тот вектор, который совпадет с вектором легитимного абонента.

Изучение процесса коррекции ВК в классической технологии СИНС привело к обнаружению отклонения от равномерностного распределения для значений компонентов ВК (рис. 1).

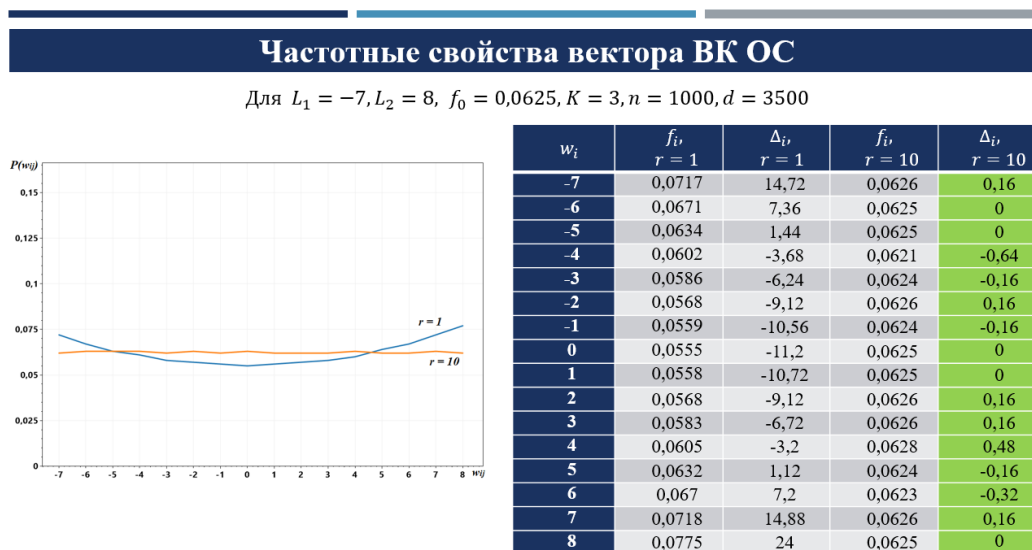


Рисунок 1. – Частотные свойства вектора весовых коэффициентов

Частоты появления значений ВК ($r = 1$) у границ интервала имеют большее значение, что дает криптоаналитику возможность выполнить атаку полного перебора с элементами

частотного анализа. При анализе комбинированного метода с секретной модификацией выявлено, что предложенный метод формирует вектор ВК ($r=10$) с более равномерным распределением вероятностей. Более точные расчеты отклонения частот от равномерного распределения приведены на рисунке 1. Относительные отклонения составляют доли процентов.

Основными характеристиками, позволяющими оценивать успешность и безопасность формирования общего секрета, следует считать вероятность удачной синхронизации сетей A и B (P_{AB}), а также вероятность удачной попытки обучения сети E (P_{AE}) при выбранной продолжительности синхронизации. Кроме вероятностей P_{AB} и P_{AE} для анализа процесса синхронизации будет полезно использовать показатель корреляционной зависимости между векторами w^A , w^B и w^A , w^E . Если сравнивать две последовательности десятичных чисел длиной $n \times K$, составляющих компоненты ВК двух векторов, то их схожесть можно оценить количеством совпадающих чисел в этих последовательностях n^c . Применительно к рассматриваемым векторам – n_{AB}^c и n_{AE}^c .

С учетом выбранных показателей безопасности и определенными базовыми значениями параметров ИНС ($L=8, K=3, n=1000$) в классической технологии наиболее приемлемыми являются вероятности успешного формирования общего секрета $P_{AB}=0,958$ и его безопасности $P_{AE}=0,054$.

В комбинированном методе с секретной модификацией за счет функции свертки криптостойкость ФОС увеличивается и принимает значение $P_{AE}=4,5 \times 10^{-7}$ при заданном количестве тактов синхронизации 3000. Но так как данный метод не требует синхронизации до полного совпадения значений ВК и процесс синхронизации останавливается на 2000 тактов безопасность общего секрета принимает значение $P_{AE}=1,02 \times 10^{-12}$.

Анализ динамики среднего числа совпадающих битов показал, что уже при $d > 2000$ показатель корреляции $\overline{n_{AB}^{cb}}/b$, где b – длина БП в битах, приближается к 1, в то время как $\overline{n_{EA}^{cb}}/b$ близко к 0,5, что свидетельствует о слабой связи векторов ВК ИНС A и ИНС B (рис. 2).

Корреляция бинарных последовательностей A с B и A с E после усиления секретности								
d	P_{AB}	P_{EA}	$P_{AB,r}$	$P_{EA,r}$	$\overline{n_{AB}^{cb}}/b$	$\overline{n_{EA}^{cb}}/b$	$\overline{n_{AB,r}^{cb}}/b$	$\overline{n_{EA,r}^{cb}}/b$
500	0	0	0	0	0,6307	0,6106	0,5065	0,5039
1000	0	0	0	0	0,7479	0,6625	0,5458	0,5159
1500	0,006	0	$7,7 \cdot 10^{-12}$	0	0,8896	0,6801	0,6713	0,5202
2000	0,295	0,004	0,0022	$1,02 \cdot 10^{-12}$	0,9711	0,6633	0,8804	0,5134
2500	0,741	0,033	0,2234	$3,9 \cdot 10^{-8}$	0,9942	0,6497	0,9750	0,5097
3000	0,958	0,054	0,8069	$4,5 \cdot 10^{-7}$	0,9989	0,6465	0,9964	0,5087

$$n = 1000, K = 3, L_1 = -7, L_2 = 8, r = 5.$$

Рисунок 2 – Анализ безопасности формируемого общего секрета

Кроме фактора безопасности формируемого секрета, необходимо учитывать и фактор допустимой продолжительности синхронизации. Очевидно, что в силу простоты программной реализации используемых ИНС, чисто вычислительные процедуры занимают незначительное время, однако результат вычислений на каждом такте синхронизации должен передаваться по каналу связи, т.е. число обменов информацией зависит от d . Вопрос о конкретном

допустимом значении d зависит от технической реализации ИНС и канала связи, но тем не менее при любой реализации очевидно, что чем меньше будет число обменов информацией, тем выше быстродействие и надежность технологии. Таким образом в комбинированном методе с секретной модификацией за счет проведения синхронизации до d_{yc} быстродействие метода увеличивается как минимум на 1000 тактов по отношению к классической технологии. А дальнейшие исследования показывают, что даже при самой слабой корреляции согласуемых БП число итераций на пятом этапе метода в среднем не превышает 7, что обеспечивает большую безопасность и сокращает количество обменов информацией по каналу связи.

Инвертирование определенного количества бит на 4 этапе метода позволяет существенно повысить криптостойкость формирования общего секрета. Возможные атаки строятся на базе отложенного перебора и подробно рассмотрены в [5]. Вероятность атаки прямого попадания в вектор ВК с проведенным инвертированием равна $P_{op1} \approx 4,3 * 10^{-3613}$. А вероятность атаки перебора синхронизаций в вектор ВК, полученный на 3 этапе и последующим перебором инвертированных битов равна $P_{op2} \approx 2,75 * 10^{-151}$.

Заключение

Рассмотренный метод формирования общего секретного числа с помощью СИНС обеспечивает высокую криптостойкость, соизмеримую с криптостойкостью современных алгоритмов симметричного шифрования, при относительно простой реализации и может использоваться как метод распределения ключевой информации абонентам сети без применения классических односторонних функций.

Литература

1. Kinzel, W. Neural Cryptography / W.Kinzel, / I. Kanter // 9th International Conference on Neural Information Processing, Singapore, 2002.
2. 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.
3. 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.
4. Голиков, В.Ф. Формирование общего секрета с помощью искусственных нейронных сетей / В.Ф. Голиков, М.Л. Радюкевич // Системный анализ и прикладная информатика. – 2019. – № 2. – С. 49–56.
5. Радюкевич М.Л. Комбинированный метод формирования криптографического ключа с секретной модификацией результатов синхронизации искусственных нейронных сетей // Системный анализ и прикладная информатика. – 2021. – № 3. – С. 51–58.
6. Радюкевич, М.Л. Усиление секретности криптографического ключа, сформированного с помощью синхронизируемых искусственных нейронных сетей / М.Л. Радюкевич, В.Ф. Голиков // Информатика. – 2020. – Т. 17, № 1. – С. 75–81. <https://doi.org/10.37661/1816-0301-2020-17-1-75-81>.
7. Радюкевич М.Л., Голиков В.Ф. Комбинированный метод формирования криптографического ключа с помощью синхронизируемых искусственных нейронных сетей. Доклады БГУИР. 2021; 19(1): 79–87.
8. Радюкевич, М.Л. Программная модель для статистического моделирования результатов исследования синхронизируемых искусственных нейронных сетей / М.Л. Радюкевич // Технические средства защиты информации: тез. докладов XX Белорус.-рос. науч.-техн. конф., Респ. Беларусь, Минск, 7 июня 2022 г. / [редкол.: Т. В. Борботько и др.]. – Минск, 2022. – С. 84–85.
9. Голиков, В.Ф. Атака на синхронизируемые искусственные нейронные сети, формирующие общий секрет, методом отложенного перебора / В.Ф. Голиков, А.Ю. Ксенович // Доклады БГУИР. – 2017. – № 8. – С. 48–53.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ПОМОЩНИК СПЕЦИАЛИСТУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

И.Н. МАСЛАК, А.Ю. КУЛАЖЕНКО

РУП «Производственное объединение «Белоруснефть»

Стремительное развитие инновационных технологий открывает новые горизонты в развитии бизнеса и получении конкурентных преимуществ. Вместе с тем порождает новые риски и угрозы как для самого внедрения, так и для дальнейшей работы заказчика. Например, с каждым годом все острее стоит вопрос информационной безопасности, причем абсолютно на всех уровнях. И вся сложность заключается в том, что для поиска уязвимостей и кибератак используются все те же современные технологии BigData, искусственный интеллект [1].

Зачастую основное внимание ИБ-специалистов уделяется внешнему периметру. Тем не менее существует вероятность того, что злоумышленник преодолет системы безопасности внешнего периметра и окажется внутри сети. Таких методов существует огромное количество, включая социотехнические, используя манипулирование психологией человека, линейностью его действий или иными факторами. Внутренняя защита обычно сводится к разделению прав и антивирусной защите – либо от непонимания серьезности угроз и рисков, либо слабой квалификации и осведомленности технического персонала и сотрудников или недостаточного финансирования кибербезопасности.



Рисунок 1. – Карта отражающая целевой уровень зрелости ИБ и типовой текущий уровень зрелости предприятия

На рисунке 1 приведена карта, предоставленная Лабораторией Касперского, показывает целевой уровень зрелости ИБ и типовой текущий уровень зрелости предприятия.

Информационная безопасность не может быть обеспечена «навсегда»; обеспечение информационной безопасности представляет собой непрерывный процесс анализа угроз, инцидентов и организации реагирования на них.

Процесс обеспечения информационной безопасности должен быть систематическим и интегрированным в бизнес-процессы организации.

Технологии искусственного интеллекта влияют на все сферы нашей жизни, включая кибербезопасность, а значит, и та самая нейросеть может как применяться для целевых атак и компрометации, так и помогать [2].

Анализ угроз – это процесс определения потенциальных угроз безопасности для информации и информационных систем. Он представляет собой систематический подход к идентификации и оценке угроз на основе вероятности их возникновения и воздействия на информацию и системы.

На основе результатов анализа угроз разрабатываются политики, процедуры и меры безопасности, необходимые для предотвращения или смягчения угроз. Кроме того, проведение анализа угроз должно быть периодическим, чтобы оценить новые угрозы или изменения в существующих, поскольку угрозы могут появляться и изменяться со временем.

После разработки политик и мер безопасности на основе анализа угроз необходимо проводить мониторинг и управление рисками. Мониторинг и управление рисками представляют собой непрерывный процесс, который включает в себя оценку эффективности мер безопасности и принятие дополнительных мер, если это необходимо.

Важным аспектом обеспечения информационной безопасности является также обучение и осведомление сотрудников. Сотрудники организации должны понимать оценку рисков и принимать участие в обеспечении безопасности. Для этого организации проводят обучение и различные мероприятия по повышению осведомленности сотрудников, связанные с информационной безопасностью и заботой о конфиденциальности.

Таким образом, обеспечение информационной безопасности представляет собой непрерывный цикл, который включает в себя анализ угроз, планирование и реализацию мер безопасности, мониторинг и управление рисками, а также обучение и осведомление сотрудников.

Мероприятия по повышению осведомленности сотрудников являются важным компонентом обеспечения информационной безопасности. Ниже приведены основные мероприятия по повышению осведомленности сотрудников:

1. Обучение информационной безопасности – проведение тренингов и семинаров по вопросам безопасности информации, в том числе установка комплекса правил обращения с информацией, защиты паролей, модернизация ПО.

2. Формирование культуры безопасности информации – сознательное отношение к личным данным сотрудника, обучение правилам безопасного обращения с информацией, отчетности о потенциальных угрозах с конфиденциальной информацией.

Допустим, что наша организация заботится о безопасности данных и хочет создать виртуальный тренажер для обучения сотрудников культуре безопасности информации.

Поэтому предоставим запрос искусственному интеллекту о создании сценария виртуального тренажера:

1. Первый этап: Введение.

Сотрудники будут ознакомлены с основами безопасности информации и понятиями, связанными с этой темой. В этом разделе будут представлены понятия, такие как угрозы для безопасности, конфиденциальность, доступность и целостность.

2. Второй этап: Спам и фишинг.

В этом разделе сотрудникам будут представлены техники защиты от спама и фишинга. Работники организации узнают, как распознать нежелательную переписку, не переходить по подозрительным ссылкам и не открывать вложения от незнакомых отправителей. Кроме того, сотрудники будут учиться использованию специализированных программ для защиты электронной почты.

3. Третий этап: Удостоверение личности.

В этом разделе сотрудники будут учиться, как запрашивать удостоверение личности для обеспечения безопасности при работе с конфиденциальной информацией. Сотрудники узнают, как проверять достоверность каждого запрашиваемого документа, чтобы гарантировать, что информация не будет передана злоумышленникам.

4. Четвертый этап: Хранение данных.

В этом разделе сотрудникам будут представлены техники безопасного хранения данных, такие как пароли и зашифрование. Сотрудники будут учиться созданию более комплексных и безопасных паролей, а также использованию инструментов для защиты информации, хранящейся на личных компьютерах и портативных устройствах.

5. Пятый этап: Сложный вопрос.

Здесь будет представлен сложный сценарий, связанный с реальной угрозой для безопасности информации. Сотрудники будут обучены, как трактовать и обрабатывать эту угрозу, а также как предотвратить подобные атаки в будущем [3].

Каждый этап содержит теоретическую и практическую части, которые позволяют удобнее воспринимать информацию и запоминать ее. Внедрение такого виртуального тренажера может значительно повысить уровень культуры безопасности в организации.

Надлежащее выполнение вышеперечисленных мероприятий помогает развивать культуру безопасности информации в организации и снизить риски возникновения угроз.

Заключение

Искусственный интеллект является мощным инструментом в создании виртуальных тренажеров и симуляций для обучения культуре безопасности информации. ИИ может быть использован для анализа поведения пользователей и создания индивидуальных программ обучения, которые оптимизируют процесс обучения и позволяют сотрудникам эффективно усваивать информацию.

Литература

1. Управление рисками на IT-проектах: что поменялась за последние годы [Электронный ресурс] / Режим доступа: <https://habr.com/ru/companies/T1Holding/articles/374671/> – Дата доступа 9.04.2023.

2. Не шути с ChatGPT. Как хайповая нейросеть может применяться в кибератаках и изменить ИБ [Электронный ресурс] / Режим доступа: <https://habr.com/ru/companies/kaspersky/articles/725730/> – Дата доступа 16.04.2023.

3. ChatGPT [Электронный ресурс] / Режим доступа: <https://chat.openai.com/> – Дата доступа 30.03.2023.

ЗАЩИТА ОТ ПРИНУЖДЕНИЯ В СИСТЕМАХ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

М.А. КАЗЛОВСКИЙ

Государственное предприятие «НИИ ТЗИ»,
г. Минск, Республика Беларусь

Введение

В последние десятилетия повсеместно наблюдается тренд на цифровизацию различных общественных процессов. В том числе предпринимаются попытки по переводу в цифровое пространство процесса голосования избирателей на выборах. За это время было разработано множество разнообразных систем электронного голосования, однако лишь малая часть из них использовались при проведении выборов государственного масштаба. Более того, даже использованные системы, как правило, применялись для голосования лишь небольшого числа избирателей.

Процедура проведения электронного голосования хоть и схожа с процедурой проведения обычного офлайн-голосования, имеет ряд преимуществ. В частности, при грамотно организованном электронном голосовании создаются криптографические доказательства корректности проведения важных для голосования процессов: аутентификации избирателя и выдача ему бюллетеня, получения от избирателя заполненного бюллетеня, подсчета полученных бюллетеней и др. Соответственно, такие угрозы обычного голосования как регистрация в качестве избирателей несуществующих или не имеющих права голоса лиц, вбросы в ящик для голосования лишних бюллетеней и некорректный подсчет голосов блокируются.

Однако для систем электронного голосования необходимо учитывать другие угрозы, возникающие из-за особенностей организации голосования. К таким угрозам можно отнести уязвимость клиента для голосования (устройство, с помощью которого избиратель принимает участие в голосовании, может быть заражено вредоносным программным обеспечением, способным нарушить анонимность избирателя и даже модифицировать содержание бюллетеня), возможность продажи голоса (избиратель может доказать как именно он проголосовал третьему лицу с целью продажи голоса) и принуждение избирателя (третье лицо может вынудить избирателя проголосовать определенным образом, не голосовать вовсе или отдать необходимые для голосования данные). На наш взгляд, именно наличие подобных угроз, является одной из основных причин, сдерживающих развитие электронного голосования. Данная статья посвящена анализу криптографических механизмов безопасности, которые позволят обеспечить защиту от принуждения избирателя.

1. Понятие защиты от принуждения в литературе

Фундаментальной работой, в которой впервые было сформулировано понятие «защита от принуждения» является статья [1]. В ней рассматривается такое свойство систем электронного голосования, как *свобода выбора* (receipt-freeness) – неспособность избирателя доказать противнику, что он проголосовал определенным образом, даже если сам избиратель желает получить такое доказательство. Выполнение данного свойства означает, что система защищена от атаки, в ходе которой противник требует от избирателя предоставления криптографического доказательства содержания бюллетеня. Однако выполнение этого свойства не защищает систему от ряда других атак:

1. атаки рандомизации – противник принуждает избирателя отдавать свой голос случайным образом (например, использовать случайно составленный бюллетень);
2. атаки воздержаний – противник может установить личности проголосовавших избирателей и, соответственно, вынудить их не принимать участия в голосовании;
3. атаки симуляции – противник вынуждает избирателя раскрыть полученный после этапа регистрации личный (секретный) ключ до начала этапа голосования, что позволит противнику выдать себя за легитимного избирателя.

Таким образом понятно, что даже обеспечивающая свободу выбора система, недостаточна для защиты избирателя от принуждения противником.

Авторы работы [1] вводят более сильное свойство систем электронного голосования: *защиту от принуждения* (coercion-resistant). Выполнение данного свойства гарантирует, что противник не сможет определить выполнил ли принуждаемый избиратель его требования, в частности: проголосовать определенным образом, отправить случайный бюллетень, не голосовать вовсе или раскрыть использующийся для подачи голоса личный (секретный) ключ. Интуитивно ясно, что невозможно обеспечить защиту от принуждения, если противник контролирует избирателя на протяжении всех этапов голосования. Поэтому в системах, которые обеспечивают защиту от принуждения, возможности противника всегда будут ограничены. Например, в [1] авторы ограничивают противника следующими предположениями:

1) большая часть регистраторов (субъектов, которые проводят аутентификацию избирателя и выдают ему необходимые для голосования данные) и большая часть счетчиков (субъектов, которые выполняют обработку и подсчет бюллетеней) не контролируются противником и не сотрудничают с ним;

2) противник может заставить избирателя сохранить информацию, которую избиратель отправляет регистратору или получает от регистратора, а также может заставить избирателя использовать определенные данные в процессе регистрации;

3) противник не имеет возможности контролировать процедуру регистрации, а также выполняется по крайней мере одно из следующих трех предположений:

- избиратель не может сохранить полученную в ходе регистрации информацию для передачи ее противнику (например, для регистрации используется смарт-карта);

- с противником не взаимодействует ни один из регистраторов;

- избиратели точно знают, какие регистраторы сотрудничают с противником;

4) подача голоса выполняется по анонимному каналу связи (чтобы противник не смог связать отправленный в систему бюллетень с конкретным избирателем).

В процессе регистрации пользователь проходит аутентификацию перед регистратором, получая от него секрет, который также регистрируется на публичной доске в зашифрованном на общем открытом ключе счетчиков виде. На этапе голосования избиратель тоже включает в состав бюллетеня зашифрованный на общем открытом ключе счетчиков секрет. В этом случае, при принуждении избиратель может раскрыть противнику несуществующий, но неотличимый от настоящего секрет. При подсчете голосов все бюллетени подвергаются криптографическому перемешиванию, после чего счетная комиссия отклоняет бюллетени, для которых указаны несуществующие секреты (путем их сравнения с помощью механизма «plaintext equivalence test» с зашифрованными зарегистрированными секретами). Поэтому раскрыв несуществующий секрет противнику, избиратель может использовать зарегистрированный секрет для анонимного голосования, причем противник не сможет установить, голосовал ли данный избиратель повторно.

Описанный выше механизм является первым подходом, который может использоваться для защиты от принуждения. Помимо [1], он в том или ином виде реализован в системах, которые описаны в работах [2, 3, 4, 5]. В дальнейшем будем называть его *использованием несуществующего секрета*. Существует альтернативный механизм защиты от принуждения, основанный на использовании системы электронного голосования, дизайн которой позволяет избирателю отправлять организаторам голосования несколько бюллетеней. После завершения этапа голосования, доверенная третья сторона выполнит конфиденциальную фильтрацию поданных бюллетеней, то есть удалит все поступившие от одного избирателя бюллетени, кроме последнего. При этом процесс фильтрации организован таким образом, что он не раскрывает информацию о том, какие именно бюллетени были удалены. Примеры таких систем описаны, например, в работах [6, 7, 8]. Этот механизм будет в дальнейшем называть *использованием переголосования*.

2. Анализ защиты от принуждения

Сравним описанные механизмы с использованием несуществующего секрета и с использованием переголосования по ряду критериев:

1. Требование по отсутствию принуждения на этапе регистрации характерно только для механизма с использованием несуществующего секрета.

2. Необходимость иметь устройство для безопасного хранения учетных данных характерна только для механизма с использованием несуществующего секрета.

3. Необходимость обманывать противника характерна только для механизма с использованием несуществующего секрета.

4. Требование по отсутствию доступа к устройствам аутентификации избирателя у противника характерно как для механизма с использованием несуществующего секрета, так и для механизма с использованием переголосования.

5. Требование по отсутствию принуждающего в какой-то момент на этапе голосования характерно как для механизма с использованием несуществующего секрета, так и для механизма с использованием переголосования.

6. Требования по отсутствию принуждающего в конце этапа голосования характерно для механизма с использованием переголосования.

Таким образом, можно видеть, что оба указанных механизма имеют свои преимущества и недостатки в ряде критериев.

При этом мы считаем, что введенные в [1] допущения слабо соответствуют действительности, то есть могут быть выполнены только в абстрактной, не связанной с реальной жизнью системе. Это убеждение следует из того, что логика электронного голосования предполагает полную открытость и прозрачность, то есть все описание процесса голосования, исходные коды программного обеспечения, которое планируется использовать в процессе голосования, и прочие элементы голосования, должны быть публично раскрыты за некоторое время до начала процесса. Соответственно, у противника будет достаточно возможностей, чтобы разработать стратегию, которую можно использовать для эффективного принуждения избирателей. Принуждение не сработает на этапе голосования – не проблема, противник потребует проходить этап регистрации под его контролем, а значит, механизма с использованием несуществующего секрета не сработает. Для реализации механизма с использованием переголосования необходимо, чтобы противник не контролировал избирателя в конце этапа голосования – противник сделает все, чтобы проголосовать последним.

В этой ситуации очевидно, что классические криптографические механизмы, которые предполагается использовать для защиты от принуждения, окажутся неработоспособными. Поэтому необходимо предложить некоторую модель принуждения, которая будет явно указывать на возможности принуждающего и эти возможности или не будут противоречить положению дел в реальном мире, или не будут оторваны от реальности. Можно выделить основные характеристики процесса принуждения:

1. Уровень огласки, то есть насколько принуждение явное и есть ли возможность у принуждаемого сформировать доказательства процесса принуждения. Чем более заметны действия, которые выполняет принуждающий, тем ниже шанс на проведение такого принуждения.

2. Простота обнаружения. Если процесс принуждения может быть легко обнаружен внешним наблюдателем, то шанс на проведение такого принуждения невысок.

3. Количество вовлеченных в процесс принуждения людей и объем трудозатрат. Чем выше эти числа, тем ниже шанс на успешную атаку.

Уровень опасности принуждения мы предлагаем определять исходя из канала, через который оно выполняется: 1 уровень – нет принуждения; 2 уровень – принуждения через виртуальный канал; 3 уровень – принуждения через физический канал.

Заключение

1. Защита от принуждения является важным свойством для систем электронного голосования.

2. Для обеспечения защиты от принуждения может использоваться один из двух механизмов: использованием несуществующего секрета или использование переголосования.

3. Оба механизма имеют как свои преимущества, так и свои недостатки. При этом для их корректного применения должны выполняться требования, которые трудно реализовать в реальной системе электронного голосования.

4. Необходимо предложить и обосновать альтернативное определение защиты от принуждения, которое соответствует реальным возможностям противника.

Литература

1. Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-resistant electronic elections. In WPES, 2005.

2. Ben Adida. Helios: Web-based Open-audit Voting. In USENIX, 2008.

3. Sergiu Bursuc, Gurchetan S Grewal, and Mark D Ryan. Trivitas: Voters Directly Verifying Votes. In VOTE-ID, 2012.

4. Jeremy Clark and Urs Hengartner. Selections: Internet Voting with Over-the-Shoulder Coercion-Resistance. In FC, 2012.

5. Michael R. Clarkson, Stephen Chong, and Andrew C. Myers. Civitas: Toward a secure voting system. In S&P, 2008.

6. Wouter Lueks, Iñigo Querejeta-Azurmendi, and Carmela Troncoso. VoteAgain: A scalable coercion-resistant voting system, 2020.

7. Philipp Locher, Rolf Haenni, and Reto E Koenig. Coercion-Resistant Internet Voting with Everlasting Privacy. In FC, 2016.

8. Dirk Achenbach, Carmen Kempka, Bernhard Löwe, and Jörn Müller-Quade. Improved Coercion-Resistant Electronic Elections through Deniable Re-Voting. USENIX Journal of Election Technology and Systems, 2015.

ЗАСЕДАНИЕ № 5

НОРМАТИВНО-ПРАВОВОЕ И КАДРОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 004.056.5

СИСТЕМА ПОДГОТОВКИ КАДРОВ ПО СПЕЦИАЛЬНОСТИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Т.В. БОРБОТЬКО

*Белорусский государственный университет информатики и радиоэлектроники,
Минск, 220013, Беларусь*

Информационные технологии играют важнейшую роль в обеспечении бизнес-процессов различных организаций, производственной деятельности многих предприятий и в жизнедеятельности человека. Вместе с тем их широкое использование в повседневной деятельности человека обуславливает появление широкого спектра рисков [1]. Ключевыми проблемами современности становятся обеспечение безопасности информационной инфраструктуры государства и предприятий, совершенствование мер защиты национальных интересов Республики Беларусь в информационной сфере. Существующее положение дел обуславливает необходимость и совершенствование подготовки кадров в сфере информационной безопасности с учетом современных угроз информационной безопасности.

Для противодействия подобным угрозам необходимо обеспечить формирование соответствующей системы подготовки кадров, которая должна затрагивать не только классические направления, связанные с образовательным процессом в университетах, а также повышения квалификации специалистов, но и отбор мотивированных кадров для последующего их обучения в вузах, а самое главное – формирования основы для развития культуры обеспечения информационной безопасности, как приоритетной цели и внутренней потребности человека, приводящей к осознанию личной ответственности и к самоконтролю при выполнении работ, влияющих на информационную безопасность.

Система подготовки кадров должна охватывать следующие аудитории обучающихся: школьники, студенты, специалисты ответственные в организациях за обеспечение информационной безопасности, руководители различных подразделений, обеспечивающие критически важные процессы в организациях с применением информационных технологий, сотрудники организаций – пользователи информационных систем. Назначение системы подготовки кадров – обеспечение требуемого уровня квалификации специалистов и достижения ими высокой эффективности в процессе трудовой деятельности, что в итоге влияет на обеспечение стабильности бизнес-процессов организаций.

Функции системы, следующие:

1. Информационная. Ее реализация заключается в способствовании формированию представления о сфере и направлениях информационной безопасности у молодежи, что должно способствовать появлению интереса к направлению и мотивации выпускника школы в выборе будущей профессии.

2. Образовательная. Обеспечивает формирование знаний, умений, навыков и готовность их использования в трудовой деятельности выпускниками университетов.

3. Повышение осведомленности. Эта функция направлена на совершенствование знаний сотрудников организаций в области информационной безопасности с учетом текущего положения дел в этой сфере.

Указанная система подготовки кадров по специальности «Информационная безопасность» создана в Белорусском государственном университете информатики и радиоэлектроники (БГУИР) в партнерстве с рядом организаций и учреждений Республики Беларусь.

Работа со школьниками ведется в рамках такого проекта университета как Академия информатики для школьников, который реализуется при Институте информационных технологий БГУИР. С 2019 года в указанном проекте открыто направление «Кибербезопасность» и осуществляется набор школьников. В рамках направления сформированы две образовательные программы «Безопасность персональных данных» и «Безопасность информационных сетей». Первая программа является базовой, а вторая углубленной. В рамках лекционных и практических занятий школьники получают знания и практические навыки по обеспечению безопасности информации, которая хранится и обрабатывается на персональных компьютерах, а также передается в информационных сетях.

С сентября 2022 года в Учреждении образования «Национальный детский технопарк» функционирует направление «Информационная безопасность» в рамках которого, реализуется образовательная программа для школьников «Обеспечение безопасности информации в информационных системах». В рамках программы, обучающиеся получают базовые знания и навыки в области информационной безопасности, а также выполняют исследовательские проекты.

С 2023 года в БГУИР будет осуществляться набор студентов для обучения по специальности 6-05-0611-02 «Информационная безопасность» профилизации «Защита информации в телекоммуникациях». В рамках профилизации студенты получают знания и практические навыки по инженерно-технической защите объектов, противодействию утечки информации по техническим каналам, защиты информации в информационных системах и криптографической защите информации. Выпускник в дальнейшем имеет возможность получить углубленное высшее образование, закончив магистратуру по специальности 7-06-0611-02 «Информационная безопасность» профилизации «Защита информации в информационных системах». Обучение по указанной специальности является логическим продолжением подготовки специалиста и затрагивает вопросы обеспечения кибербезопасности информационных систем. По указанной специальности в магистратуре образовательный процесс реализуется также и в заочной форме.

Совместно с Международным центром образования, созданным на базе Государственного предприятия «Национальный центр обмена трафиком» и Национальным центром защиты персональных данных Республики Беларусь реализуются программы повышения квалификации по технической и криптографической защите информации. Это позволяет сотрудникам кафедры защиты информации проводить апробацию новых образовательных программ для последующего использования их материалов в учебном процессе кафедры в рамках университета, а также поддерживать непосредственную связь с заказчиками кадров и своевременно актуализировать содержание учебных дисциплин по специальности «Информационная безопасность».

Литература

1. Концепция информационной безопасности Республики Беларусь, утвержденная Постановлением Совета Безопасности Республики Беларусь № 1 от 18 марта 2019 г.

Авторы

Борботько Тимофей Валентинович, д.т.н., профессор, заведующий кафедрой защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

Адрес для корреспонденции

220013, Республика Беларусь,
г. Минск, П. Бровки, 6,
учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»
тел. +375293341812 (A1);
Email: secure@bsuir.by
Борботько Тимофей Валентинович

АКТУАЛЬНЫЕ ВОПРОСЫ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.В. МАРЧЕНКО

Уважаемые участники конференции!

В настоящее время, характеризующееся взрывным ростом информационного противоборства так называемого коллективного запада и Российской Федерации, особо актуальным становится предотвращение использования информационных технологий для решения задач, противоречащих интересам обеспечения мира и стабильности, суверенитета, безопасности государства и его граждан.

В решении данного вопроса руководством страны определено в качестве одного из основных и главных направлений – кадровое обеспечение информационной безопасности.

Вопросы совершенствования подготовки кадров в области информационной безопасности ежегодно рассматриваются на совещаниях и заседаниях, организуемых Советом Безопасности Российской Федерации, на которых принимаются важные решения.

В настоящее время Минобрнауки России, Минцифры России, Минтрудом России, ФСТЭК России и другими заинтересованными федеральными органами исполнительной власти активно ведется работа по реализации основного концептуального документа – Концепции развития кадрового обеспечения в области информационной безопасности в Российской Федерации на долгосрочную перспективу, реализуемой в период с 2017 по 2025 год.

Проблематике решения вопросов совершенствования подготовки кадров в области информационной безопасности было посвящено оперативное совещание Совета Безопасности Российской Федерации, состоявшееся под руководством Президента Российской Федерации 2 декабря 2022 г.

В решении задач, поставленных оперативным совещанием, активно работает ФСТЭК России во взаимодействии с другими федеральными органами исполнительной власти, прежде всего ФСБ России, Минобрнауки России и Минцифры России.

Так, в соответствии с подготовленным Минобрнауки России и ФСТЭК России Типовым отраслевым планом целевой подготовки кадров в области информационной безопасности федеральными органами исполнительной власти и государственными корпорациями, осуществляющими нормативное правовое регулирование в областях (отраслях), в которых функционируют объекты критической информационной инфраструктуры, разрабатываются свои отраслевые планы целевой подготовки кадров в области информационной безопасности на 2023–2028 годы.

Минобрнауки России активно ведутся работы по усилению механизмов государственной аккредитации и лицензирования образовательной деятельности образовательных организаций, созданию системы многофункциональных учебно-научных (производственных) центров по проблемам информационной безопасности в федеральных округах на базе ведущих образовательных организаций высшего образования.

На завершающем этапе находится подготовка ФСТЭК России внесения изменений в ведомственный нормативный правовой акт, направленных на задействование специалистов со средним профессиональным образованием в области информационной безопасности для защиты объектов критической информационной инфраструктуры Российской Федерации.

Уважаемые участники конференции, коллеги!

Требования к наличию в государственных органах и организациях Российской Федерации должностных лиц и подразделений, отвечающих за обеспечение информационной безопасности, к квалификации специалистов по защите информации определены в ряде нормативных правовых актах:

- Указе Президента Российской Федерации от 1 мая 2022 г. № 250;
- постановлениях Правительства Российской Федерации № 1272, 399, 79, 171, 333;
- приказах ФСТЭК России № 33 и 235;

– профессиональных стандартах в области информационной безопасности, а также в других нормативных правовых актах.

Требования к квалификации включают в себя требования к уровню образования специалистов по защите информации (высшему и дополнительному профессиональному образованию), стажу работы на должности, связанной с обеспечением безопасности информации, а также периодичности прохождения повышения квалификации указанными специалистами.

И чтобы соответствовать указанным требованиям руководители государственных органов и организаций принимают меры по профессиональной переподготовке и повышению квалификации своих специалистов по защите информации.

Уважаемые участники конференции, коллеги!

В 2016 году ФСТЭК России была определена центром ответственности по формированию предложений о контрольных цифрах приема по специальностям и направлениям подготовки укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность» за счет бюджетных ассигнований федерального бюджета.

Работа, проводимая ФСТЭК России по данному направлению во взаимодействии с заинтересованными федеральными органами исполнительной власти, позволяет формировать предложения, на основе которых Минобрнауки России ежегодно определяются контрольные цифры приема на соответствующие учебные годы.

На слайде № 4 отображена информация по данному вопросу и, как видно из него, динамика объема контрольных цифр приема имеет стабильную тенденцию роста.

В целях определения контрольных цифр приема граждан по специальностям и направлениям подготовки «Информационная безопасность» ФСТЭК России ежегодно направляет соответствующие запросы в федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, организации оборонно-промышленного комплекса, основные финансово-кредитные организации и организации, оказывающие услуги в области защиты информации.

Полученные результаты позволяют характеризовать текущее состояние кадрового обеспечения в области информационной безопасности, его количественную и качественную структуру.

Общее количество работников, занятых в этой области в указанных государственных органах, организаций на 1 января 2022 года составляет величину более 45 700 человек.

Необходимо отметить, что эффективность решаемых задач по защите информации существенно зависит от качества подготовки специалистов в этой области и приобретенной ими квалификации.

В настоящее время состав работников, которые имеют высшее образование по специальностям и направлениям подготовки «Информационная безопасность» или прошли переподготовку в указанной области, составляет в среднем около 40 %, и это невысокий показатель. Недостаточный уровень компетентности работников при проведении работ по защите информации, наряду с другими факторами, является причиной невыполнения требований по защите информации.

Положительным необходимо отметить, что в организациях оборонно-промышленного комплекса практически большая часть специалистов по защите информации с непрофильным базовым образованием за период 2018 – 2022 годов прошли повышение квалификации.

В то же время, несмотря на обязательность профессиональной переподготовки должностных лиц из руководящего состава, а также повышения квалификации государственных гражданских служащих в органах власти недостаточно внимания уделяется данному вопросу.

Мы надеемся, что данная проблема будет разрешена в результате поэтапного выполнения требований постановлений Правительства Российской Федерации от 5 мая 2016 г. № 399 «Об организации повышения квалификации специалистов по защите информации

и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса», а также от 15 июля 2022 г. № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)».

На основе анализа сведений о кадровом обеспечении органов власти, органов местного самоуправления, организаций оборонно-промышленного комплекса и организаций, оказывающих услуги в области защиты информации, определены предварительные данные о потребностях в специалистах по защите информации, которые представлены на слайде № 6.

Прогнозные значения потребности в специалистах на 2023–2025 годы будут использованы при разработке предложений по корректировке контрольных цифр приема граждан на обучение за счет бюджетных ассигнований федерального бюджета по указанным специальностям.

Уважаемые участники конференции, коллеги!

Взрывной рост информационного противоборства «Коллективного Запада» и Российской Федерации, политика беспрецедентного санкционного давления, происходящие с начала специальной военной операции, привели к тому, что руководством страны принимаются меры по выходу из болонской системы образования.

В соответствии с изданным Указом Президента Российской Федерации от 12 мая 2023 г. № 343 «О некоторых вопросах совершенствования системы высшего образования» определено проведение в 2023/2024 и 2025/2026 учебных годах проведение пилотного проекта по организации обучения в шести образовательных организациях высшего образования по следующим уровням высшего образования: базового высшего образования (с обучением 4–6 лет), специализированного высшего образования (с обучением в магистратуре от 1 до 3 лет) и уровня профессионального образования – аспирантуры.

В целях реализации Указа Президента Российской Федерации активно, в том числе при участии ФСТЭК России, ведется работа по разработке ФГОС ВО нового поколения, основных профессиональных образовательных программ, актуализация и разработка новых программ дополнительного профессионального образования в области информационной безопасности. До начала обучения по новым образовательным программам в области ИБ с 1 сентября текущего года в образовательных организациях ВО, определенных Указом (Балтийский федеральный университет Э. Канта, Московский авиационный институт, Томский государственный университет), ФСТЭК России необходимо будет оперативно подготовить предложения для установления Минобрнауки России контрольных цифр приема для указанных образовательных организаций.

Уважаемые участники конференции!

Сейчас мне хотелось бы проинформировать кратко о принимаемых мерах ФСТЭК России по направлению совершенствования кадрового обеспечения в области информационной безопасности с учетом наделенных Службе Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 полномочиями.

В рамках реализации этих полномочий ФСТЭК России:

– участвует в разработке нормативных правовых актов, методических документов, регламентирующих сферу образования в области информационной безопасности;

– разрабатывает квалификационные требования к специалистам, работающим в области противодействия иностранным техническим разведкам, технической защиты информации и обеспечения безопасности информации в ключевых системах информационной инфраструктуры;

– проводит работу по разработке примерных программ дополнительного профессионального образования по вопросам ТЗИ и обеспечения безопасности значимых объектов критической информационной инфраструктуры РФ, осуществляет рассмотрение и согласование программ подготовки, профессиональной переподготовки и повышения квалификации специалистов по защите информации, представляемых в Службу образовательными организациями.

В целях методического обеспечения профессиональной переподготовки и повышения квалификации специалистов, работающих в области ПД ИТР, ТЗИ и обеспечению безопасности значимых объектов критической информационной инфраструктуры

Службой разработаны и утверждены 4 примерные программы профессиональной переподготовки и 12 примерных программ повышения квалификации специалистов, а также методические рекомендации по разработке программ дополнительного профессионального образования.

Должен отметить, что указанные методические документы очень востребованы и активно используются образовательными организациями при разработке своих рабочих дополнительных профессиональных программ.

В настоящее время ФСТЭК России разработаны проекты еще трех программ дополнительного профессионального образования и проект методических рекомендаций по рассмотрению (экспертизе) проектов программ дополнительного профессионального образования в области защиты информации. В ближайшее время данные документы будут утверждены и рекомендованы образовательным организациям для использования.

В рамках имеющихся полномочий, а также приказа Минобрнауки России от 19 октября 2020 г. № 1316 ФСТЭК России осуществляет рассмотрение и согласование проектов программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области информационной безопасности.

По нашему мнению, работа, проводимая Службой в этом направлении, необходима. Ведь эффективность подготовки специалистов по защите информации, необходимые для работы специалистам компетенции, знания и навыки во многом зависят и от качества и актуальности образовательных программ, реализуемых образовательными организациями.

Как видно из информации, представленной на слайде, динамика объема представления в ФСТЭК России программ дополнительного профессионального образования на рассмотрение и их согласование Службой имеет также устойчивую тенденцию роста.

Согласованные Службой и утвержденные образовательными организациями программы профессиональной переподготовки и повышения квалификации в области информационной безопасности включаются в Перечень согласованных ФСТЭК программ, который размещен на официальном сайте ФСТЭК России в информационно-телекоммуникационной сети «Интернет» (*раздел «Техническая защита информации», подраздел «Обучение специалистов»*).

В настоящее время в указанный Перечень включено более 600 программ дополнительного профессионального образования от 206 образовательных организаций.

В целях совершенствования системы подготовки, профессиональной переподготовки и повышения квалификации специалистов по защите информации территориальными органами ФСТЭК России проводится работа по координации деятельности совещательных органов по подготовке указанных специалистов, созданных в каждом федеральном округе.

Во взаимодействии с совещательными органами, а также региональными учебно-методическими объединениями высшего образования по укрупненной группе направлений и специальностей 10.00.00 «Информационная безопасность» управлениями ФСТЭК России по федеральным округам проводится работа по оказанию методической помощи образовательным организациям по разработке рабочих программ профессиональной переподготовки и повышения квалификации специалистов по защите информации в соответствии с примерными образовательными программами, утвержденными ФСТЭК

России, информируется образовательное сообщество об изданных новых нормативных правовых актах по ПД ИТР, ТЗИ и обеспечению безопасности значимых объектов КИИ.

ФСТЭК России также осуществляет обеспечение образовательных организаций нормативными правовыми актами и методическими документами в области защиты информации.

Уважаемые участники конференции, коллеги!

Проводимая ФСТЭК России в рамках своих полномочий работа по методическому руководству подготовкой, переподготовкой и повышением квалификации специалистов, работающих в области ПД ИТР, ТЗИ и обеспечения безопасности значимых объектов критической информационной инфраструктуры, а также реализации документов и нормативных правовых актов, принимаемых во исполнение решений оперативного совещания Совета Безопасности Российской Федерации от 6 декабря 2022 г., будет и в дальнейшем направлена на совершенствование системы подготовки указанных специалистов и повышение уровня кадрового обеспечения в области информационной безопасности.

По нашему глубокому убеждению, только хорошо продуманная, взвешенная и совместная работа всех заинтересованных государственных органов, организаций и образовательного сообщества позволит эффективно и своевременно решать вопросы совершенствования кадрового обеспечения в области информационной безопасности.

МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПЕРЕДАЧЕ ИНФОРМАЦИИ В МИКРОЭЛЕКТРОННЫХ СИСТЕМАХ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

К.А. БОЧКОВ, С.Н. ХАРЛАП

*Белорусский государственный университет транспорта,
г. Гомель, 246653, Республика Беларусь*

В последнее время значение информационной безопасности для автоматизированных систем управления технологическими процессами (АСУ ТП) значительно возросло. При этом следует учитывать, что для автоматизированных систем управления ответственными технологическими процессами (АСУ ОТП), где информационная безопасность может влиять на показатели функциональной безопасности, обеспечение выполнения требований информационной безопасности имеет ряд особенностей. Необходимость учета требований информационной безопасности при разработке АСУ ОТП привело к тому, что актуальными стали вопросы, связанные со взаимодействием методов обеспечения функциональной и информационной безопасности.

В настоящее время сложилась ситуация, когда ряд нормативных документов в области функциональной безопасности систем железнодорожной автоматики и телемеханики (ЖАТ) в некоторых случаях устанавливают требования, которые традиционно относят к информационной безопасности. Например, технический регламент Таможенного союза ТР ТС 003/2011 «О безопасности инфраструктуры железнодорожного транспорта» (в редакции 2021 года) [1] определяет системы ЖАТ как «Автоматизированные системы оперативного управления технологическими процессами, связанными с обеспечением безопасности движения и информационной безопасности», т.е. не разделяет системы, связанные с функциональной и информационной безопасностью. Для подтверждения соответствия требованиям ТР ТС 003 таких систем применяются одни и те же нормативные документы, в которых наряду с требованиями функциональной безопасности к программному обеспечению предъявляются классические требования информационной безопасности: защита от несанкционированного доступа, контроль целостности программ и данных, отсутствие недеklarированных возможностей (например, п. 4.7.6 ГОСТ 33894 «Системы железнодорожной автоматики и телемеханики на железнодорожных станциях. Требования безопасности и методы контроля» [2]). Таким образом, граница между требованиями информационной и функциональной безопасности становится нечеткой. Более того, становится невозможным подтвердить соответствие требованиям функциональной безопасности без выполнения ряда требований информационной безопасности.

В настоящее время эта проблема систем ЖАТ решается последовательным выполнением сначала мероприятий по обеспечению функциональной безопасности (испытаний, верификации ПО и т.д.), а затем реализацией процедур защиты информации поверх мероприятий функциональной безопасности [3]. Результатом выполнения таких процедур является создание дополнительных средств защиты, которые являются внешними по отношению к средствам обеспечения функциональной безопасности – защищенной среды [4]. Такой подход является избыточным, так как методы защиты частично могут дублировать друг друга. В то же время опыт проведения испытаний и экспертиз различных систем ЖАТ говорит о том, что методы обеспечения функциональной безопасности успешно могут быть использованы и для решения задач информационной безопасности [3].

Анализ предметных областей функциональной и информационной безопасности, выполненный в [3] и [4], позволяет сделать вывод о том, что применительно к системам ЖАТ методы обеспечения функциональной безопасности позволяют достичь тех же целей, защищают те же объекты и требования к их реализации более жесткие по сравнению с аналогичными методами информационной безопасности.

Сравнение типичных угроз информационной и функциональной безопасности выполнялся на основе информации «Банка данных угроз безопасности информации» ФСТЭК России [5]. Угрозами информационной безопасности являются события, связанные с нарушением конфиденциальности, целостности и доступности обрабатываемой в АСУ ТП информации. Отличительными признаками систем управления технологическими процессами и объектами, которые определяют требования к ним, являются [6]:

- высокие требования к функциональной безопасности;
- сложность и уникальность микроэлектронных систем ЖАТ из-за прямой зависимости выполняемых ими функций от конфигурации объектов управления (станций, перегонов и т.д.);
- наличие разнообразных функциональных и конструктивных элементов и подсистем (рельсовая цепь, светофор, стрелочный электропривод и др.);
- большое количество и территориальная рассредоточенность объектов управления;
- высокие требования к надежности электропитания;
- работа в реальном масштабе времени, т.е. обеспечение минимального времени реакции на изменение внешних условий;
- наличие различных видов избыточности;
- наличие человека в контуре управления;
- широкий диапазон внешних электромагнитных помех;
- наличие ограниченного набора четко сформулированных задач;
- периодичность выполнения определенного класса технологических алгоритмов и их ярко выраженный дискретный характер;
- влияние отказов и сбоев программного обеспечения на безопасность функционирования.

Из этих особенностей следует, что актуальными для систем ЖАТ будут являться только угрозы информационной безопасности, связанные с вмешательством в нормальное функционирование системы, что значительно сокращает их перечень. Угрозы же, связанные с неправомерным случайным или преднамеренным ознакомлением пользователя с технологической информацией, которая для него не предназначена, не представляет опасности и могут быть исключены из рассмотрения.

Таким образом, угрозы информационной безопасности АСУ ТП можно классифицировать следующим образом:

1) внешние угрозы:

- несанкционированный удаленный доступ к управлению;
- вредоносное ПО;
- подмена или искажение данных от датчиков (подсистем);
- прерывание канала связи с контрольными датчиками;
- умышленное выведение из строя оборудования;
- приведение системы в состояние «отказ в обслуживании».

2) внутренние угрозы:

- несанкционированный локальный доступ к управлению;
- ошибки конфигурации оборудования;
- намеренное причинение ущерба сотрудниками;
- уязвимости в индустриальном ПО и протоколах, том числе недеklarированные возможности.

Источниками проникновения этих угроз в систему ЖАТ могут быть аппаратное обеспечение и системы передачи информации. Однако в связи с тем, что доступ к информационному оборудованию системы ЖАТ практически всегда ограничивается организационными (запираемые помещения) и техническими (физической блокировкой портов) мерами источником проникновения внешних угроз остается только система передачи информации.

Для внутренних же угроз источниками проникновения являются как аппаратное обеспечение информационного оборудования, так и системы передачи информации.

Рассмотрим методы защиты систем передачи информации, применяемые в рамках обеспечения функциональной безопасности, и их влияние на информационную безопасность. Основным нормативным документом, определяющим требования к обеспечению безопасной передачи информации, является ГОСТ Р МЭК 62280-2017 [7].

Для того чтобы не нарушались требования безопасной передачи информации необходимо, чтобы принятое сообщение обладало следующими свойствами: достоверность, целостность, последовательность и актуальность. В соответствии с этим стандартом определены следующие угрозы функциональной безопасности для систем передачи информации:

- повторение старого (неактуального) сообщения;
- удаление сообщения;
- вставка сообщения в информационный поток от другого источника;
- переупорядочивание (изменение последовательности сообщений в информационном потоке);
- повреждение (изменение сообщения в формально корректное другое сообщение);
- задержка сообщения;
- подмена (реальный отправитель сообщения отличается от ожидаемого отправителя).

Сравнение рассмотренных выше угроз информационной и функциональной безопасности для систем передачи информации приведено в таблице 1.

Таблица 1. – Сравнение угроз информационной и функциональной безопасности

Угрозы информационной безопасности	Угрозы функциональной безопасности							
	Повторение	Удаление	Вставка	Переупорядочивание	Повреждение	Задержка	Подмена	Другое
Несанкционированный удаленный доступ к управлению	+	+	+	+	-	-	+	-
Вредоносное ПО	+	+	+	+	+	+	+	-
Подмена или искажение данных от датчиков	-	-	-	-	+	-	+	-
Прерывание канала связи с контрольными датчиками	-	+	-	-	-	+	-	-
Умышленное выведение из строя оборудования	-	+	-	-	-	-	-	-
Приведение системы в состояние «отказ в обслуживании»	+	-	-	-	-	-	-	-

Как видно из таблицы, все угрозы информационной безопасности перекрываются угрозами функциональной безопасности, поэтому никаких дополнительных мероприятий по защите информации в системах передачи данных не требуется.

В стандарте также определены три категории систем передачи информации:

– категория 1: закрытые системы передачи, которые разработаны для известного и фиксированного максимального числа участников, все основные свойства системы передачи информации известны и постоянны на протяжении времени жизни системы. Система позволяет контролировать несанкционированные подключения с высокой степенью достоверности, риск несанкционированного доступа в таких системах незначителен;

– категория 2: открытые системы передачи, свойства которых неизвестны, частично неизвестны или изменяются на протяжении времени жизни системы, возможности для расширения группы пользователей ограничены, группа или группы пользователей известны, риск злонамеренной атаки, можно считать незначительным;

– категория 3: открытые системы передачи, в которых существует возможность вредоносной атаки и для которых требуются криптографические меры защиты.

Системы ЖАТ в подавляющем большинстве относятся к первой категории систем передачи информации (за исключением систем, использующих радиоканал, которые относятся к третьей категории). Для систем первой категории согласно таблице 2. В ГОСТ Р МЭК 62280-2017 [7] основной угрозой является повреждение сообщений, а угрозой подмены сообщений можно пренебречь ввиду наличия незначительной возможности для несанкционированного доступа.

Стандарт рекомендует к применению следующий перечень методов защиты:

- a) порядковый номер;
- b) временная метка;
- c) тайм-аут;
- d) идентификаторы источника и пункта назначения;
- e) сообщение обратной связи;
- f) процедура идентификации;
- д) код защиты;
- h) криптографические методы.

При этом для систем передачи категории 1 достаточен следующий сокращенный перечень, по–поддерживающий требуемый уровень безопасности:

- идентификаторы источника и/или адресата (в случае больше, чем одного отправителя, и/или больше, чем одного получателя);
- порядковый номер и/или временные метки в объеме, необходимом приложению;
- код защиты.

Каждый метод может обеспечить защиту от одной или нескольких угроз при передаче сообщений. Для обеспечения требуемого уровня безопасности необходимо продемонстрировать, что существует по крайней мере один соответствующий метод или комбинация методов для каждого вида угроз (таблицы 2–3).

Таблица 2. – Матрица угроз функциональной безопасности и методов защиты

Угрозы функциональной безопасности	Методы защиты							
	порядковый номер	временная метка	тайм-аут	идентификаторы	обратная связь	идентификация	код защиты	криптографические методы
Повторение	+	+	–	–	–	–	–	–
Удаление	+	–	–	–	–	–	–	–
Вставка	+	–	–	+	+	+	–	–
Переупорядочивание	+	+	–	–	–	–	–	–
Повреждение	–	–	–	–	–	–	+	–
Задержка	–	+	+	–	–	–	–	–
Подмена	–	–	–	–	+	+	–	+

Таблица 3. – Матрица угроз информационной безопасности и методов защиты

Угрозы информационной безопасности	Методы защиты							
	порядковый номер	временная метка	тайм-аут	идентификаторы	обратная связь	идентификация	код защиты	криптографические методы
Несанкционированный удаленный доступ к управлению	+	+	-	+	+	+	-	+
Вредоносное ПО	+	+	+	+	+	+	+	+
Подмена или искажение данных от датчиков	-	-	-	-	+	+	+	+
Прерывание канала связи с контрольными датчиками	+	-	+	-	-	-	-	-
Умышленное выведение из строя оборудования	+	-	-	-	-	-	-	-
Приведение системы в состояние «отказ в обслуживании»	+	+	-	-	-	-	-	-

Таким образом, рассмотренные в стандарте угрозы функциональной безопасности и меры защиты для систем передачи информации перекрывают все возможные угрозы информационной безопасности и являются достаточными для их нейтрализации.

Выводы

Предметная область информационной безопасности АСУ ТП все более полно интегрируется в предметную область функциональной безопасности, что подтверждается включением классических требований, угроз и методов защиты информационной безопасности в стандарты по функциональной безопасности. Поэтому метод последовательного выполнения мероприятий по обеспечению сначала функциональной, затем информационной безопасности, рекомендованный ГОСТ Р 59505-2021 [4] и приводящий к созданию дополнительной внешней защищенной среды, является неэффективным. Такой подход является избыточным, так как методы защиты дублируют друг друга.

Более перспективной является интеграция требований информационной безопасности в требования функциональной безопасности на ранних стадиях жизненного цикла. Работы предлагается выполнять параллельно, все конфликты должны при этом разрешаться с приоритетом функциональной безопасности (рис. 1).



Рисунок 1. – Взаимодействие функциональной и информационной безопасности

При этом для исключения дублирования работ подтверждение соответствия требованиям функциональной и информационной безопасности желательно проводить в одной организации, аккредитованной в этих областях.

Литература

1. Технический регламент Таможенного союза ТР ТС 003/201 «О безопасности инфраструктуры железнодорожного транспорта» (редакция 2021 года). – БелГИСС, 2022 – 35 с.
2. ГОСТ 33894 – 2016 «Системы железнодорожной автоматики и телемеханики на железнодорожных станциях. Требования безопасности и методы контроля». – Москва: Стандартинформ, 2017. – 27 с.
3. Бочков К.А., Харлап С.Н., Буй П.М. Обеспечение информационной и функциональной безопасности микроэлектронных систем железнодорожной автоматики и телемеханики на соответствие требованиям нормативных документов // Комплексная защита информации: материалы XXVII научно-практической конференции, 24–26 мая 2022 г., – Москва, Медиа Группа «Авангард», 2022. – С. 173–183.
4. ГОСТ Р 59505-2021 Измерение, управление и автоматизация промышленного процесса. Основные принципы обеспечения функциональной безопасности и защиты информации. – Москва: Стандартинформ, 2021 – 27 с.
5. Банк данных угроз безопасности информации // <https://bdu.fstec.ru/threat>. – Дата доступа: 26.04.2023.
6. Бочков, К.А. Микропроцессорные системы автоматики на железнодорожном транспорте: учеб. пособие / К.А. Бочков, А.Н. Коврига, С.Н. Харлап. – Гомель: БелГУТ, 2013. – 254 с.
7. ГОСТ Р МЭК 62280-2017. Железные дороги. Системы связи, сигнализации и обработки данных. Требования к обеспечению безопасной передачи информации. – Москва: Стандартинформ, 2014. – 49 с.

ПРИМЕНЕНИЕ ИНТЕРАКТИВНЫХ СРЕД МОДЕЛИРОВАНИЯ В ЦЕЛЯХ ПОВЫШЕНИЯ КИБЕРУСТОЙЧИВОСТИ ОТРАСЛЕВЫХ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР

Е.Л. ГЕНГРИНОВИЧ

*Акционерное Общество «Информационные технологии и коммуникационные системы»,
г. Москва, Российская Федерация*

Введение

Парадигма «холодной войны» и связанной с ней гонки вооружений постепенно переросла в «виртуальную войну» и соперничество за доминирование в информационном пространстве [1].

С другой стороны, по результатам опроса руководителей служб безопасности более 400 ведущих мировых корпораций, почти 40 % опрошенных, не полностью уверены в том, что их персонал достаточно квалифицирован и сможет справиться с кибератаками, если таковые случатся завтра. Более 30 % заявили, что они проводят обучение по информационной безопасности раз в год, причем 65 % времени приходится на просмотр слайдов Power Point. Все признали, что часто упускается из виду существование потребности в обучении всего персонала в организациях, а не только профильных специалистов. [2]

Мировые рынки быстро отреагировали на новые реалии, связанные с ростом угроз по информационной безопасности. По данным агентства Гартнер, 15 % компаний в корпоративном секторе уже используют специализированные продукты для оценки уязвимостей информационной инфраструктуры и развития практических навыков своих специалистов по информационной безопасности. Под такими специализированными продуктами имеются в виду платформы, построенные на основе интерактивных сред моделирования (Гартнер: Cyber Range). По аналогии с применением тренажеров для обучения сил специального назначения и пилотов, использование интерактивных сред моделирования (ИСМ) позволяет создать цифровой двойник информационной инфраструктуры, имитирующий широкий спектр сценариев, связанных с компьютерными инцидентами. Лаборатории по информационной безопасности, на основе ИСМ в настоящее время создаются правительствами, корпорациями, университетами и коммерческими центрами обучения.

Один из лидеров Российского рынка информационной безопасности, группа компаний ИнфоТеКС, сублимировала накопленный опыт по защите информационных инфраструктур, в «коробочном» ИСМ-решении – Киберполигон Amprige. Для многих термины Киберполигон, ИСМ все еще достаточно абстрактны, что часто бывает, когда новая развивающаяся технология только начинает получать широкое распространение на рынке. Поэтому стоит более детально описать перечень задач, решаемых с их помощью.

1. Основные термины и определения

Киберполигон (на основе ИСМ) – платформа для разработки, доставки и использования интерактивных сред моделирования. Где среда моделирования – это представление ИТ, АСУТП, мобильных и киберфизических систем, приложений и инфраструктур организации, включая варианты сценариев атак, разнообразных типов пользователей и их действий, а также любых других интернет-служб, публичных или частных сервисов. Платформа формирует киберпространство, которое включает комбинацию технологий, необходимых для реализации и использования среды моделирования, а также дополнительных компонент, которые, в свою очередь, желательны или необходимы для достижения конкретных целей применения киберполигона [1].

Киберустойчивость – способность предвидеть, противостоять, восстанавливаться и адаптироваться к неблагоприятным условиям, стрессам, компьютерным атакам или компрометации систем, включающих информационные ресурсы [1].

Кибервозможности – это ресурсы и активы, позволяющие государству/корпорациям обеспечивать влияние на противников или конкурентов, путем использования кибератак, и соответственно, защиту от аналогичных внешних угроз [1].

Цифровая адаптивность (Gartner: Digital Dexterity) – способность и желание использовать существующие и новые технологии для достижения бизнес-результатов [1].

Захват флага (Capture The Flag – CTF) – соревнования для специалистов по информационной безопасности для выявления новых талантов и восполнения пробелов в практических навыках.

2. Функциональная архитектура киберполигонов на основе ИСМ

На рисунке 1 приведены общие архитектурные компоненты и связанные с ними функции киберполигона. Функциональная архитектура не обязательно должна включать все компоненты, однако, в зависимости от целей его использования, определенные функции могут считаться желательными или даже де-факто обязательными. Если эти функции изначально не поддерживаются киберполигоном, то необходима его интеграция с программными решениями третьих производителей.

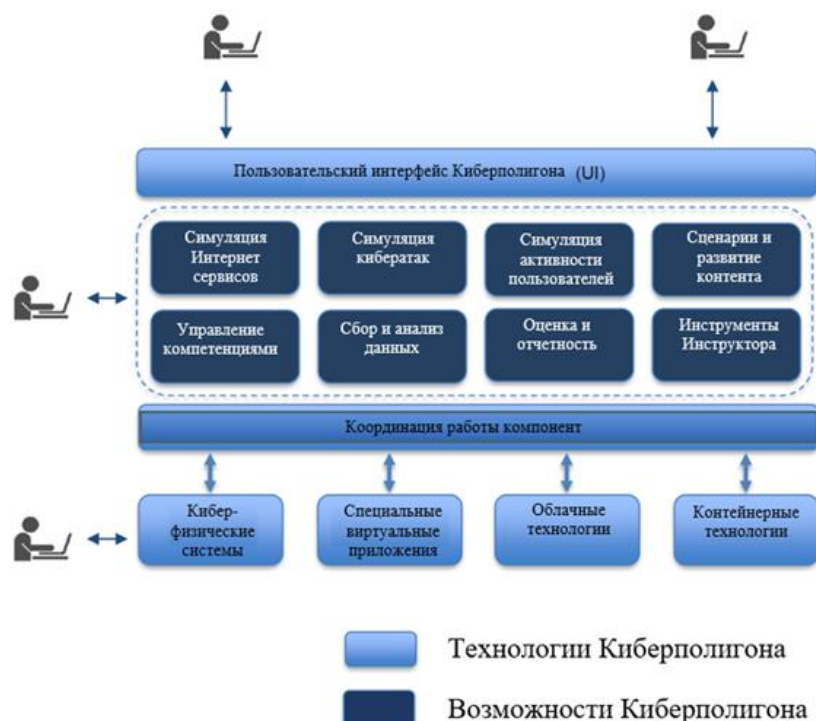


Рисунок 1. – Комплексная функциональная архитектура киберполигона

3. Варианты применения

Варианты применения киберполигонов развиваются с течением времени, в соответствии с изменениями в технологиях и возрастающей важностью информационной составляющей в процессах цифровизации бизнеса. Важно определить, понятные на сегодня, задачи, решаемые с использованием киберполигона, а не конкретные функции, возможности или даже технологии, которые лучше всего подходят для каждого варианта применения.

Начнем с определения категорий пользователей, которые могут решать задачи с использованием киберполигонов:

- корпорации (частные и государственные);
- лица, принимающие стратегические решения (частные и государственные);
- специалисты по информационной безопасности;
- военнослужащие, входящие в состав киберподразделений;
- специалисты операционных центров безопасности (SOC);
- преподаватели;

- студенты;
- исследователи;
- организаторы мероприятий.

Варианты применения киберполигонов можно свести в таблицу, где каждому варианту сопоставлен базовый функциональный набор.

Таблица 1. – Матрица функциональных наборов для различных вариантов применения

Функции	Варианты применения									
	Тестирование ИБ	Исследование ИБ	Формирование компетенций ИБ	Обучение ИБ	Развитие кибервозможностей	Повышение киберустойчивости	Оценка компетентности	Набор персонала	Цифровая адаптивность	Соревнования ИБ
Координация работы компонент			☞	☞	☞	☞	☞	☞	☞	☞
Симуляция интернет-сервисов						☞				
Симуляция атак	☞	☞	☞	☞	☞	☞	☞			☞
Симуляция пользователей сети		☞			☞	☞				
Управление компетенциями			☞	☞	☞	☞	☞	☞		☞
Создание сценариев			☞	☞	☞	☞	☞	☞		☞
Сбор и анализ данных		☞	☞	☞	☞	☞		☞		☞
Оценка и отчетность			☞	☞	☞	☞	☞	☞		☞
Инструменты Инструктора			☞	☞	☞	☞	☞			

Рассмотрим более подробно решаемые задачи для каждого из упомянутых вариантов применения.

3.1. Обучение информационной безопасности

Одна из постоянных жалоб со стороны работодателей – отсутствие практического опыта у молодых выпускников ИТ/ИБ специальностей. Основная причина, то что до появления киберполигонов, получение студентами практического опыта ИБ было практически нерешаемой задачей. По этой причине университеты, колледжи и даже школы по всему миру, начали рассматривать варианты использования киберполигонов в учебном процессе.

3.2. Повышение киберустойчивости

В целом, термин киберустойчивость применим к любому процессу, системе, бизнесу и организации, где эксплуатируют ИТ, АСУ, АСУТП, IoT. В контексте киберустойчивости,

киберучения предоставляют организациям возможности проверить реальный уровень готовности реагировать на киберинциденты и степень эффективности использования людей, процессов и технологий для защиты критически важной информации, услуг и активов. Анализ результатов киберучений и принятие корректирующих мер, позволит организации значительно повысить свою киберустойчивость.

3.3. Тестирование безопасности

Наряду с исследованиями в области безопасности, это наиболее традиционный вариант использования киберполигонов, когда тестируются симуляция информационной инфраструктуры, на которой проводятся контролируемые атаки с целью выявления потенциальных уязвимостей перед развертыванием и использованием.

3.4. Исследование безопасности

Киберполигон – это фундаментальное средство для проведения исследований в области безопасности в широком спектре областей информационной безопасности. По самой своей природе киберполигоны разрабатываются для исследования новых методов обнаружения и предотвращения атак, эмуляции вредоносных программ и многого другого.

3.5. Повышение компетентности

Обучение по вопросам ИБ, сегодня, проводится как в режиме онлайн, так и очно. В обоих случаях большая часть обучения происходит путем прослушивания видео или живых лекций, а также путем чтения заметок или слайдов. Обучение практическим навыкам либо отсутствует совсем, либо занимает ничтожно мало времени. Использование киберполигонов меняет ситуацию в корне и обеспечивает удобный и экономичный способ проведения практического обучения, а также оценки знаний и различных сертификаций.

3.6. Развитие кибервозможностей

Кибервозможности совпадают с компетенциями профессионалов ИБ. В таком контексте киберполигоны являются частью кибервозможностей страны и могут использоваться для развития ее киберпотенциала, в части исследований и разработки киберинструментов и других активов, а также проведения киберучений для проверки работоспособности этих разработок. В контексте развития цифровой экономики, киберполигоны могут обеспечивать крупномасштабные киберучения с участием сотен тысяч человек.

3.7. Оценка компетентности

Компетентность – это набор атрибутов, таких как знания, навыки и умения, необходимые для успешного выполнения конкретных задач. Поскольку растет, как число задач, связанных с ИБ, так и требуемый уровень квалификации специалистов для их решения, организациям требуется эффективный способ проведения переаттестаций персонала. Использование киберполигонов позволит организациям выполнять более точную оценку компетентности, на основании не только традиционных теоретических тестов, но и оценивать наличие практических навыков, предлагая выполнение задач ИБ на эмуляции реальной сети и наблюдая за поведением испытуемого, в процессе их решения.

3.8. Прием сотрудников на работу

Поскольку для оценки компетентности появилась возможность использовать киберполигоны, то следует ожидать также изменения в процессе найма персонала, что позволит организациям лучше выявлять, проверять и нанимать подходящих кандидатов.

3.9. Цифровая адаптивность

Традиционные методологии разработки программного обеспечения и передовые практики безопасности рекомендуют использовать различные среды, такие как разработка, подготовка и производство. В связи с продолжающейся цифровой трансформацией и требованиями к поддержке множества коммуникационных и бизнес-задач организациям приходится проецировать одни и те же инновационные практики на разные задачи,

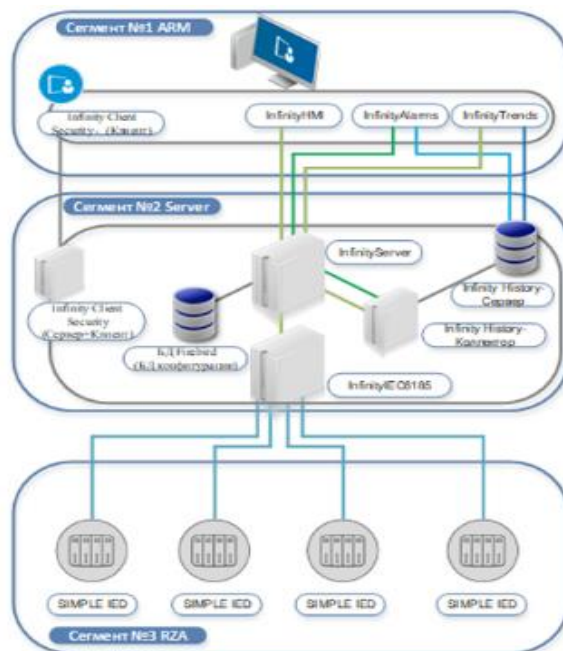
одновременно поддерживая более быстрые жизненные циклы разработки. Киберполигон обеспечит возможность отработки этих практик в виртуальном окружении и сформирует у персонала необходимые навыки для их практического последующего применения в инфраструктуре организации.

3.10. Национальные и международные соревнования ИБ

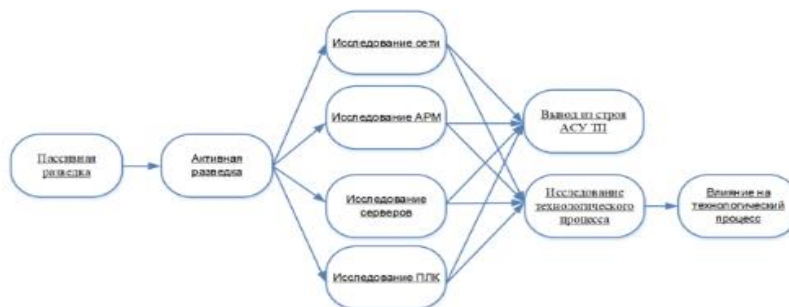
Многие страны организуют национальные соревнования ИБ, которые обычно проводятся в формате «Захват флага» (Capture The Flag – CTF). Киберполигоны меняют способ организации таких соревнований, позволяя проводить более масштабные мероприятия и более реалистичные симуляции. Яркими примерами таких соревнований являются European Cyber Security Challenge, Word Skills и CyberStars.

4. Синергия при взаимодействии с вузами (на примере НИУ МЭИ)

Цифровые подстанции (ЦПС), создаваемые в соответствии с МЭК 61850, в состав которых входят современные терминалы релейной защиты и автоматики (РЗА) – это сложная компьютерная система и объект критической информационной инфраструктуры, в то же время.



Этапы сценариев атак:



- Проприетарное взаимодействие
- МЭК-61850 MMC
- OPC DA
- OPC AE
- OPC HAE
- OPC HDA

Рисунок 2. – Шаблон инфраструктуры ЦПС для Киберполигона Amprige

В тесном сотрудничестве с кафедрой РЗА НИУ МЭИ разрабатываются цифровые двойники различных архитектур ЦПС (рис. 2), проводится анализ уязвимостей и проверка сценариев обеспечения информационной безопасности.

Применение Киберполигона позволило обеспечить поддержку работ кафедры РЗА НИУ МЭИ по разработке новых алгоритмов расчета коэффициента готовности⁴ терминала РЗА на основе комбинации полумарковского процесса⁵ и моделирования угроз информационной безопасности.

Заключение

Киберполигон Amprige позволяет имитировать набор возможных атак на реплику «целевой информационной инфраструктуры». Виртуальная инфраструктура может включать в себя сеть, хранилище, компьютеры (серверы), RTU, шлюзы IoT, IP-камеры, а также коммутаторы, маршрутизаторы, брандмауэры, модели технологических процессов и т.д. Платформа содержит компоненты управления обучением. С ее помощью как инструкторы, так и стажеры выполняют задачи в рамках predetermined информационных сценариев. Помимо обучения, платформа полезна для экспериментов с новыми технологиями, проверки новых идей и наблюдения за тем, как команды взаимодействуют с новыми решениями информационной безопасности. Активно развивается направление поддержки отраслевых задач (ТЭК, индустрия, транспорт, телеком, интернет вещей, медицина и других).

Amprige успешно применяется более чем в 10 российских вузах и учебных центрах. В этом году он был приобретен Испытательным центром ПАО «Россети». Ведутся переговоры еще с рядом вузов и крупных корпораций.

Инвестиции только в технологии не приносят необходимого эффекта, пора сосредоточиться на людях.

Литература

1. ESCO WG5 Paper “Understanding Cyber Ranges: From Hype to Reality, 2020.
2. Report “Cyber crisis response failing to adapt to modern threats” Osterman Research, Inc. 2020.

⁴ Коэффициент готовности – вероятность застать терминал РЗА в работоспособном состоянии в данный момент времени.

⁵ Полумарковский процесс – это случайный процесс, который переходит из одного состояния в другое в соответствии с заданными распределениями вероятностей, а время пребывания процесса в каком-либо состоянии также является случайной величиной. Его широко используют в теориях надежности и массового обслуживания.

МЕТОДЫ И МОДЕЛИ ЭФФЕКТИВНОСТИ БЕЗОПАСНОЙ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

И.Р. ШЕХОВЦОВА

*МКООО «Газпром Интернэшнл Лимитед»,
г. Калининград, Российская Федерация*

Введение

На практике ряд электронных документов может не достигать своей конечной цели в ожидаемое время, что может обернуться существенными потерями для компании [1]. Требования к надежности и безопасности автоматизированных систем управления непрерывно возрастают, и на первый план выходит проблема рациональной организации и оптимизации документопотоков [2]. Для компаний, осуществивших переход на электронный документооборот (ЭДО), задача анализа особенностей движения документов приобретает исключительную важность.

В поле компетенции системы электронного документооборота (СЭД) попадает не только решение проблем автоматизации хранения, поиска и обработки информации, но и обеспечение заданного уровня информационной безопасности (ИБ) и высокой устойчивости: для системы ЭДО вводятся такие критерии безопасности, как гарантирование достижения финала маршрута и общая безопасность системы. Иначе говоря, реализуемая СЭД должна не только автоматизировать движение документов, но и позволять делать это эффективно с точки зрения выбранного критерия.

В современных системах ЭДО электронный документ недоступен пользователю, пока к нему не придет задача его обработки. При наличии отклонений в маршруте документа, в том числе временных, документ может не достигнуть своего адресата в заданное время. В связи с этим в системе ЭДО может нарушаться доступность информации – свойство, определяющее возможность использования объекта автоматизированным субъектом по запросу (ГОСТ Р ИСО/МЭК 270001-2021, ISO/IEC 27001:2022). Отсюда и возникают требования к безопасности и надежности, предъявляемые к СЭД.

Анализ литературы [3–5] показал, что вопрос эффективного управления информационными потоками документов изучен не в полной мере. Хотя к настоящему моменту времени существует достаточно много подходов к моделированию ЭДО, начиная от теоретико-множественных и теоретико-графовых и заканчивая моделями на сетях Петри, математической модели ЭДО, которая позволила бы оптимизировать СЭД с точки зрения критериев безопасности и надежности, в опубликованных работах не представлено.

Автор полагает, что исследование маршрутов документов, которым в литературе не уделяется должного внимания, даст возможность наиболее точно определить «узкие» места системы ЭДО, ограничивающие ее устойчивость и функционирование в рамках заданного уровня информационной безопасности (ИБ).

Основная часть

При рассмотрении бизнес-процессов любой организации удобно представлять процесс так, будто переходы системы из состояния в состояние происходят под действием потоков событий. В терминах потока событий можно описать поток связанных с определенным бизнес-процессом документов. Такое описание допустимо ввиду того что:

а) поток блуждающих из состояния в состояние документов можно рассмотреть, как стационарный на интервалах рабочего времени, установленного в организации, вводя допущение, что вероятностные характеристики такого потока на указанных промежутках времени не меняются;

б) события, образующие поток, появляются в последовательные моменты времени независимо друг от друга;

в) вероятность попадания на элементарный участок времени двух или более событий пренебрежимо мала по сравнению с вероятностью попадания одного события – поток ординарен.

Целесообразно применить теорию дискретных марковских процессов с дискретным временем для моделирования поэтапного движения электронного документа определенного типа от сотрудника к сотруднику.

В каждой точке маршрута электронный документ может находиться в одном из трех состояний – «Согласовано», «Согласовано с замечаниями», «Не согласовано». Входными данными для такой модели движения документа является точное понимание возможных переходов, которые необходимо смоделировать, а также вероятности перехода из одного состояния в другое, которые представлены в виде матрицы переходов и могут быть исчислены на основании статистического анализа движения конкретного типа документа. Поглощающая марковская модель позволит оценить вероятность получения результата «Согласовано» в финальной точке маршрута.

В качестве рассматриваемого типа документа был выбран договор. Процесс его согласования может быть представлен следующим образом (рис. 1):

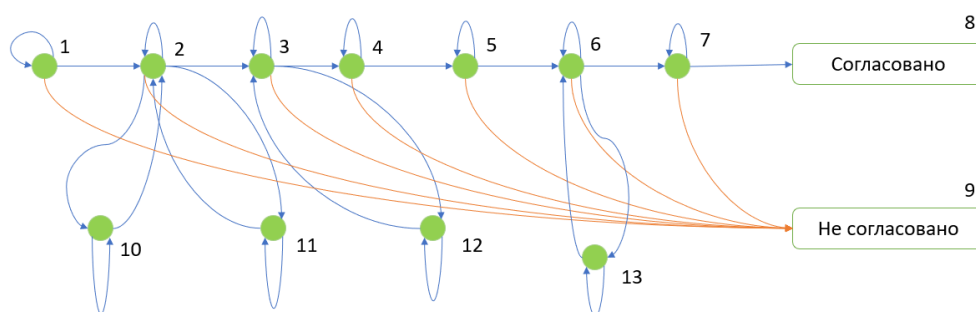


Рисунок 1. – Марковская модель согласования договора

На рисунке 1 каждой цифре соответствуют следующие этапы согласования:

- 1 – согласование непосредственным руководителем;
- 2 – согласование документа планово-экономическим управлением;
- 3 – согласование документа юридическим управлением;
- 4 – согласование руководителем корпоративной защиты;
- 5 – согласование отделом подготовки и проведения конкурентных закупок;
- 6 – согласование главным бухгалтером;
- 7 – согласование генеральным директором;
- 8 – получение результата «Согласовано»;
- 9 – получение результата «Не согласовано».

Цифрами 10, 11, 12, 13 на рисунке 1 обозначены этапы согласования сотрудниками, не предусмотренными в типовом маршруте.

В результате статистического анализа вероятностей переходов P_{ij} по каждой точке маршрута из состояния i в состояние j может быть получена матрица вероятностей переходов P размером 13×13 . Тогда вероятности состояний после k -го шага определяются рекуррентной формулой:

$$p_i(k) = \sum_{j=1}^{13} p_j(k-1)P_{ji} \quad (i = 1..13)$$

Графики зависимостей вероятностей состояний исследуемого бизнес-процесса представлены на рисунке 2: красной линией соответствует вероятность получения результата «Согласовано» в финальной точке маршрута за определенное количество дней.

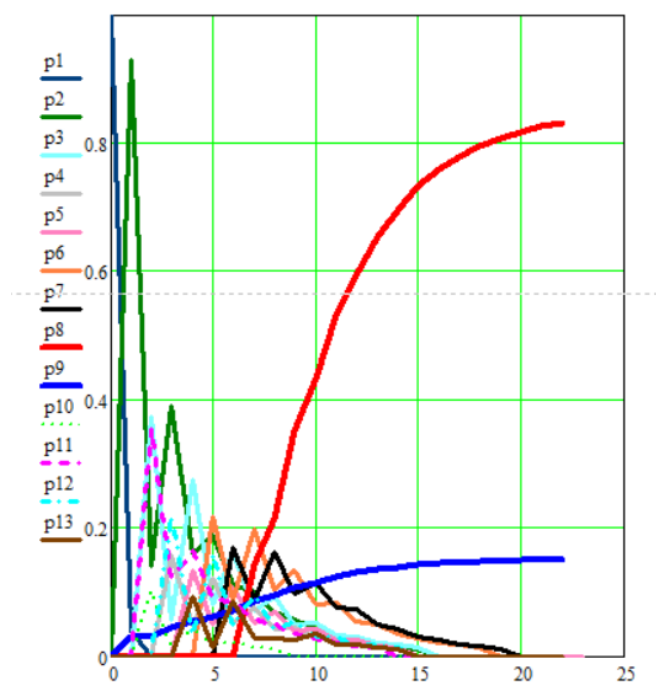


Рисунок 2. – Оценка вероятности согласования документа

Построенная модель также позволяет перейти к численной оценке рисков безопасности системы ЭДО [6]. В рамках исследуемой задачи под риском автором понимается отклонение от планируемых переходов по фиксированному маршруту. Предлагается для каждой вероятности перехода из состояния в состояние ставить в соответствие некоторую оценку, которая в дальнейшем будет называться расходом за один переход из состояния в состояние. Общий расход за какое-то количество шагов является случайной величиной, зависящей от хода бизнес-процесса. Качество оценивается величиной среднего суммарного расхода – математическим ожиданием. Тогда среднеквадратическое отклонение оцениваемого параметра системы объектов от его среднего значения (математического ожидания) и является численной оценкой риска.

Заключение

Предложенная модель позволяет обеспечить надежный и риск-ориентированный подход в принятии управленческих решений по совершенствованию современных систем ЭДО, характеризующихся высокой устойчивостью и соответствующих заданным требованиям ИБ, а также оценить эффективность безопасной системы электронного документооборота.

Литература

1. Лившиц И.И. Практика управления киберрисками в нефтегазовых проектах компаний холдингового типа. Вопросы кибербезопасности. – 2020. – № 1 (35). – С. 42–51.
2. Лившиц И.И., Соколов Е.О., Лукьянова А.А. Схемотехнические решения для практической реализации безопасного электронного документооборота. Часть 2. Новая разработка. // Газовая промышленность. – 2022. – № 11. – С. 50–70.
3. Краснянский М.Н. Проектирование информационных систем управления документооборотом научно-образовательных учреждений: монография / М.Н. Краснянский, С.В. Карпушкин, А.В. Остроух и др. – Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2015. – 216 с.
4. Гудов А.М., Завозкин С.Ю. Об одной модели оптимизации документопотоков, реализуемой при создании системы электронного документооборота // Вычислительные технологии. – 2006. – Т. 11, № S3, С. 53–67
5. Сенченко П.В. Документационное обеспечение управленческих решений / П.В. Сенченко, Ю.П. Ехлаков, В.Е. Кириенко. – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2018. – 180 с.
6. ГОСТ Р 58771-2019. Менеджмент риска. Технологии оценки риска

ПРАКТИКА НЕЗАВИСИМОГО АУДИТА БИЗНЕС-ПРОЦЕССОВ КОМПАНИИ НА БАЗЕ ЭДО

Е.О. СОКОЛОВ

*МК ООО «Газпром Интернэшнл Лимитед»,
г. Калининград, Российская Федерация*

Создание системы электронного документооборота

Известно, что для компаний, осуществивших переход на электронный документооборот (далее – ЭДО), задача обеспечения независимого аудита бизнес-процессов всех процессов «движения» документов приобретает исключительную важность [1–4]. В компании МК ООО «Газпром Интернэшнл Лимитед» (далее – Компания) в рамках реализации проекта ЭДО выполнена сквозная гибкая и бесшовная интеграция со всеми основными ИТ-системами:

- 1С Document Management версии 2.1;
- 1С Бухгалтерия версия 3 КОРП;
- 1С УХ (Управление холдингом);
- Единая система нормативно-справочной информации;
- 1С Зарплата и управление персоналом версия 3.1 КОРП.

Компания стала победителем конкурса 1С в регионе «Центральная и Восточная Европа» с проектом «Кадровый юридически значимый документооборот для компаний холдингового типа» (КЭДО) в 2022 г. Проект реализован собственным центром компетенции Компании с целью перевода в электронную форму всех нормативных, нормативно-справочных и иных типов документов, без привлечения каких-либо внешних экспертов. Система КЭДО в течение 2022 г. практически показала доступность на уровне 99,99 %, простой составил менее 3 часов. Система КЭДО зарегистрирована как программа для ЭВМ в Роспатенте.

Требования, предъявляемые к аудиту бизнес-процессов

В проекте КЭДО реализовано два контура аудитов (рис. 1):

- Внутренний контур аудита:
 - быстрый цикл
 - доработка регламентов
 - внимание руководства
 - быстрая обратная связь
- Внешний контур аудита:
 - фиксированный цикл
 - международные нормы
 - система стандартов ГОСТ Р
 - публичное решение
 - быстрая обратная связь

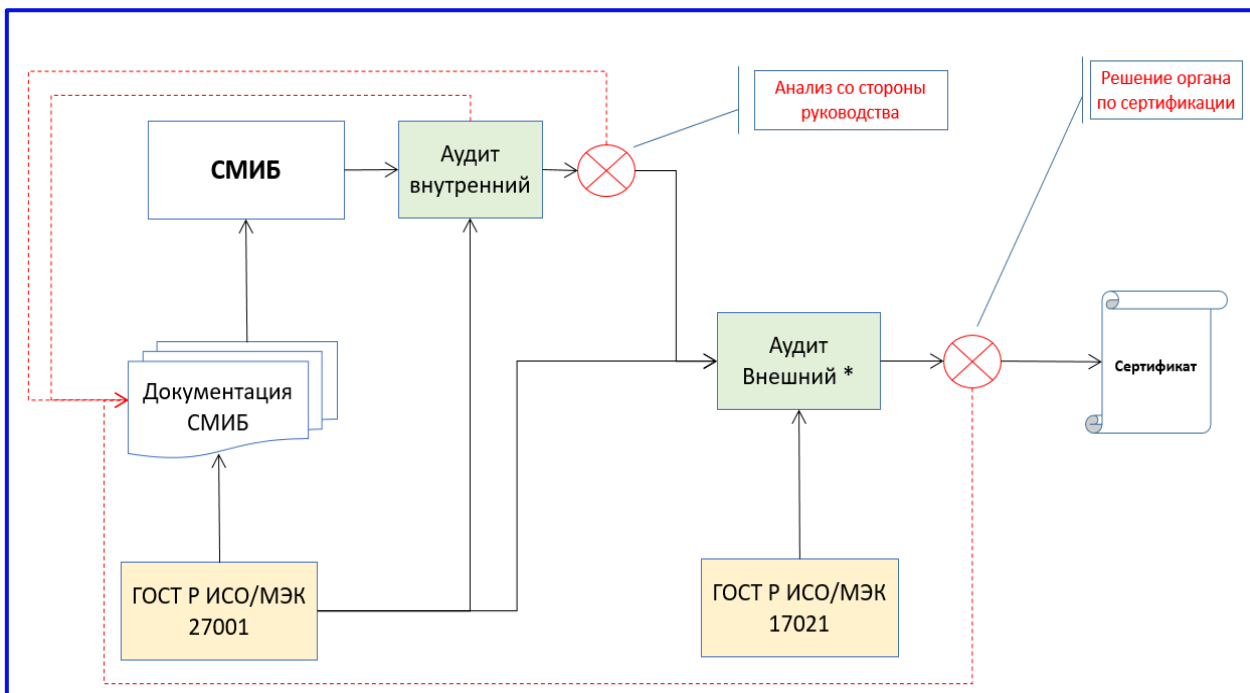


Рисунок 1. – Схема аудитов бизнес-процессов

Прохождение внешнего аудита

В проекте КЭДО реализован простой, четкий и честный план подготовки к внешнему сертификационному аудиту (рис. 2):

Задача	Дата	Статус	Ответственный		Подтверждающие документы
			Компания	Орган по сертификации	
Подготовка договора	Июль	План	A	+	Договор
GAP-аудит (внешний)	*	План	A	+	Приложение к договору
Обучение (внешнее)	*	План	A	+	Приложение к договору
Формирование команды	Июль	Выполнено	A		СЗ № 1
Обучение (внутреннее)	Август	Выполнено			СЗ № 1
Аудит (внутренний)	Август	План	A		СЗ № 1
Доработка документации	Август	План	A		СЗ № 1
Внешний аудит	Сентябрь	План	A	+	Договор
Доработка документации	Сентябрь	План	A	+	Отчет по аудиту
Выдача сертификата	Октябрь	План	A	+	Договор
Постоянное улучшение	Декабрь	План	A		План развития СМИБ на 2023 г.

Рисунок 2. – Пример плана проведения аудитов бизнес-процессов

По итогам проведения независимого международного аудита системы менеджмента информационной безопасности Компании по требованиям ГОСТ Р ИСО/МЭК 27001 оформлен сертификат (см. рис. 3).



Рисунок 3. – Сертификат на соответствие требованиям ГОСТ Р ИСО/МЭК 27001

Кроме того, можно отметить важное значение применения на практике действующего сертификата на соответствие требованиям ГОСТ Р ИСО/МЭК 27001, например, при реализации международных проектов и обеспечения соответствия иностранным требованиям в области безопасности. Пример показан далее на рисунке 4.

<ul style="list-style-type: none"> • Art. X. <u>Tout enregistrement comptable doit préciser l'origine, le contenu et l'imputation de chaque donnée ainsi que les références de la pièce justificative qui l'appuie.</u> • <u>Les éditions informatiques doivent être identifiées, numérotées et datées dès leur établissement par des moyens offrant toute garantie en matière de preuve.</u> 	<ul style="list-style-type: none"> • Ст. X Во всех бухгалтерских записях для данных должны быть указаны источник, содержание и отражение каждого элемента данных по счетам (статьям), а также ссылки на подтверждающий документ. • Такие программные записи должны быть идентифицированы, пронумерованы и датированы сразу же после их составления с помощью средств, обеспечивающих все гарантии доказательства. 	<p>Гарантии доказательства – ISO 27001</p> <p>A.18.1.3 Protection of records</p> <p>Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with <u>legislatory, regulatory, contractual and business requirements</u></p> <p>A.12.4.3 Administrator and operator logs.</p> <p>System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.</p>
--	--	--

Рисунок 4. Сертификат на соответствие требованиям ГОСТ Р ИСО/МЭК 27001

Заключение

По итогам реализации проекта аудита бизнес-процессов в Компании получены следующие объективные возможности:

- развитие собственных центров компетенции;
- расширение области сертификации по ГОСТ Р ИСО/МЭК 27001;
- сертификация по ГОСТ Р ИСО/МЭК 20000-1 и ГОСТ Р ИСО 22301;
- внутренний аудит информационной интегрированной системы менеджмента;
- обеспечение устойчивого развития.

Литература

1. Лившиц И.И. Практика управления киберрисками в нефтегазовых проектах компаний холдингового типа. Вопросы кибербезопасности. – 2020. – № 1 (35). – С. 42–51.
2. Лившиц И.И., Соколов Е.О., Лукьянова А.А. Схемотехнические решения для практической реализации безопасного электронного документооборота. Часть 2. Новая разработка / Газовая промышленность, 2022. – № 11 (840)
3. Лившиц И.И., Соколов Е.О., Лукьянова А.А. Схемотехнические решения для практической реализации безопасного электронного документооборота. Часть 1. Аналитический обзор / Газовая промышленность, 2022. – № 9 (837). – С. 40–56.
4. Лившиц И.И., Соколов Е.О., Лукьянова А.А. Расчет экономического эффекта для проекта кадрового электронного документооборота // Стандарты и качество, 2022. – № 12. – С. 67–74

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ НЕСОВЕРШЕННОЛЕТНИХ В УСЛОВИЯХ ИНФОРМАЦИОННОЙ ВОЙНЫ

Т.В. РАДЫНО

*Республиканское общественное объединение
«Белорусская научно-промышленная ассоциация»,
г. Минск, Республика Беларусь*

Информационная война – это война без правил, война без видимых разрушений и порой даже без четко определенного противника. Разнообразие применяемых в ней методов бесконечно, а ключевая опасность состоит в том, что воздействие на отдельного человека может долгое время оставаться незамеченным.

Сегодня, с применением Интернета и других средств массовой коммуникации, а также с появлением кибервойны как особого вида информационной войны, вопрос безопасности государства в информационном поле и киберпространстве становится особенно острым [1].

В рамках информационной войны неявная агрессия оказывается более существенной, чем физическая агрессия, хотя в моменты открытых вооруженных столкновений оба вида агрессии взаимно дополняют друг друга. Неявная агрессия реализуется через информационные каналы СМИ. Информация, как воплощение угрозы и манипуляции в целях достижения конкурентного превосходства над оппонентом, предстает фундаментальным оружием и мишенью информационной войны [2].

Один из наименее защищенных адресатов инфоудара – несовершеннолетние граждане: дети и подростки. В силу особенностей психофизиологического развития их оценка информации и реакция на нее может существенно отличаться от нормальной реакции взрослого, обладающего большим жизненным опытом и более устойчивой психикой. Последствия такой реакции на полученную информацию могут стать фатально-непредсказуемыми как одномоментно, так и в долгосрочной перспективе, если удар по психике ребенка будет рассчитан на его моральную и социальную деформацию.

Защита детей и подростков в условиях информационной войны, на наш взгляд, должна строиться в первую очередь путем постановки соответствующих задач государственным органам по защите подрастающего поколения от прямого доступа агрессивных масс-медиа к аккаунтам детей в интернете, ограничения доступного несовершеннолетним контента в сети Интернет, ужесточения ответственности операторов персональных данных, вплоть до блокировки ресурсов, не выполняющих требования законодательства о средствах массовой информации и о защите персональных данных, а также путем установления требований к родительскому контролю через повышение персональной ответственности родителей за действия несовершеннолетних в возрасте до 16 лет в сети Интернет.

В соответствии с пунктами 1 и 2 части первой Федерального закона Российской Федерации «О персональных данных» от 27 июля 2006 г. № 152-ФЗ (далее – Федеральный закон), персональные данные – **любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу** (субъекту персональных данных); персональные данные, разрешенные субъектом персональных данных для распространения, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных **путем дачи согласия на обработку персональных данных**, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом; оператор – государственный орган, муниципальный орган, **юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных**, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. Согласно пункту 1 части 1 статьи 6 Федерального закона,

обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных. В соответствии с частью 1 статьи 9 Федерального закона *согласие на обработку персональных данных может быть дано* субъектом персональных данных или его *представителем в любой позволяющей подтвердить факт его получения форме*, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных *полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором*.

В соответствии с абзацами восьмым, девятым и тринадцатым статьи 1 Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» (далее – Закон № 99-З), персональные данные – *любая информация, относящаяся к идентифицированному физическому лицу* или физическому лицу, которое может быть идентифицировано; оператор – государственный орган, *юридическое лицо* Республики Беларусь, иная организация, физическое лицо, в том числе индивидуальный предприниматель (далее, если не определено иное, – физическое лицо), *самостоятельно или совместно с иными указанными лицами организующие и (или) осуществляющие обработку персональных данных*; субъект персональных данных – *физическое лицо*, в отношении которого осуществляется обработка персональных данных. Согласно части второй пункта 9 Закона № 99-З, *до достижения субъектом персональных данных возраста шестнадцати лет*, за исключением вступления в брак до достижения возраста шестнадцати лет, *согласие на обработку его персональных данных дает один из его законных представителей*.

Согласно части 1 статьи 64 Семейного кодекса Российской Федерации, защита прав и интересов детей возлагается на их родителей. Родители являются законными представителями своих детей и выступают в защиту их прав и интересов в отношениях с любыми физическими и юридическими лицами, в том числе в судах, без специальных полномочий.

Согласно части первой статьи 65 Кодекса Республики Беларусь о браке и семье (далее – КоБС), семья обязана содействовать реализации прав и законных интересов членов семьи, на нее возлагается ответственность за воспитание и содержание детей, их защиту. Защита прав и законных интересов несовершеннолетних детей возлагается на их родителей, родители являются законными представителями своих несовершеннолетних детей и выступают в защиту их прав и законных интересов в отношениях с любыми лицами и организациями, в том числе в судах, без специального полномочия (часть первая и вторая статьи 73 КоБС).

Таким образом, при осуществлении доступа в Интернет несовершеннолетними родители несут ответственность за последствия такого доступа, в том числе с точки зрения вредного влияния распространяемой в глобальной сети информации. С другой стороны, операторы интернет-ресурсов, посредством которых осуществляется сбор, обработка, хранение и распространение персональных данных, обязаны обеспечить родителям возможность контроля за действиями несовершеннолетних в социальных сетях и иных ресурсах, связанных с распространением информации о частной жизни, персональных и биометрических данных, включая личные фото несовершеннолетних.

Следует отметить, что изображение человека относится к его биометрическим персональным данным (абзац второй статьи 1 Закона 99-З), поэтому использование фотографий любого гражданина особо регулируется законодательством, а тем более – ребенка. Если фотография ребенка была опубликована в интернете без согласия родителей, они вправе обратиться с жалобой в соответствующие государственные органы, а если такая публикация причинила ребенку (или его представителям) нравственные страдания, родители могут обратиться в суд с иском о возмещении морального вреда.

К лицам, нарушившим требования законодательства о персональных данных, в зависимости от конкретных обстоятельств и серьезности деяния может быть применена не

только гражданско-правовая и дисциплинарная ответственность, но также административная и даже уголовная ответственность.

Так, в соответствии с частью 2 статьи 13.11 Кодекса об административных правонарушениях (далее – КоАП) Российской Федерации, наказуема обработка персональных данных без письменного согласия субъекта, когда это необходимо, либо обработка данных с нарушением требований к составу сведений, включаемых в такое согласие, ответственность по статье 137 Уголовного кодекса (далее – УК) Российской Федерации влечет незаконное соби́рание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия; за нарушение законодательства о защите персональных данных наступает ответственность по статье 23.7 КоАП Республики Беларусь, незаконные действия в отношении информации о частной жизни и персональных данных и несоблюдение мер обеспечения защиты персональных данных образуют состав преступлений согласно статьям 203-1 и 203-2 УК Республики Беларусь.

Вместе с тем, изучение документов, опубликованных операторами и владельцами интернет-ресурсов в свободном доступе, показало, что ни Политики конфиденциальности, ни Лицензионные соглашения не содержат обязанностей операторов персональных данных, отвечающих требованиям законодательства в части обязательности проверки наличия согласия представителя несовершеннолетнего на создание последним своей странички в социальной сети и дальнейшего размещения на ней персональных данных (включая фотографии с изображением несовершеннолетних, которые относятся к особо охраняемым персональным данным), в том числе мерами уголовно-правовой охраны.

Более того, даже учреждения образования зачастую не учитывают необходимость получения согласия родителей для осуществления фото–и видеосъемки детей в учреждении образования для последующего размещения на странице социальной сети такого учреждения образования.

Так, в Республике Беларусь не требуется в случаях, предусмотренных в абзацах двадцатом статьи 6 и семнадцатом пункта 2 статьи 8 Закона 99-З, учреждению образования брать согласие на обработку персональных данных несовершеннолетних от родителей, согласно которым обработка персональных данных не требует согласия субъекта либо его законного представителя, если она является необходимой для выполнения обязанностей (полномочий) оператора персональных данных, предусмотренных законодательными актами. Ввиду того что в Кодексе об образовании и в иных нормативных правовых актах Республики Беларусь урегулированы определенные положения, на основании которых оператор (учреждение образования) осуществляет какие-либо действия с персональными данными, необходимые для осуществления образовательного процесса, учреждения образования безосновательно, на наш взгляд, распространяют свое право обрабатывать персональные данные учащихся на биометрические данные – вести фото–и видеосъемку учащихся и использовать эти материалы по своему усмотрению.

Однако, согласно пунктам 1.19 и 1.20 статьи 1 Кодекса об образовании Республики Беларусь, образовательная деятельность – это деятельность по обучению и воспитанию, **осуществляемая учреждением образования**, организацией, реализующей образовательные программы научно-ориентированного образования, иной организацией, индивидуальным предпринимателем, осуществляющими образовательную деятельность, **в ходе реализации образовательных программ**; образовательная программа – это совокупность документации, регламентирующей образовательный процесс, и требований к условиям, необходимым для получения в соответствии с ожидаемыми результатами определенного уровня основного образования или определенного вида дополнительного образования, а также специального образования. Очевидно, поскольку фото–и видеосъемка учащихся не предусмотрена образовательными программами, то она не является обязательным элементом процесса обучения, а значит, учреждение образования обязано получать согласие законных представителей несовершеннолетних, не достигших возраста

16 лет, на получение и распространение такого вида персональных данных всякий раз, когда в этом возникнет необходимость, не связанная с процессом обучения.

Защита персональных данных несовершеннолетних обеспечивает не только обеспечение нормального жизнеобеспечения подрастающего поколения, но и является одной из необходимых мер защиты суверенитета государства в части защиты его граждан от посягательств на личную и семейную безопасность. Свободный доступ недружественных информационных ресурсов к аккаунтам несовершеннолетних, незаконное собирание персональных данных несовершеннолетних, включая их биометрические данные, закладывает долгосрочные риски будущему построению общества и блокирует свободу личности в части свободы выбора ее социальной роли в государстве. Персональные данные будущих государственных деятелей должны быть надежно защищены с детства, граждане наших стран должны быть уверены, что их изображения и личные данные не будут использованы без их ведома ни в коммерческих, ни в противоправных интересах третьих лиц.

Построение Союзного государства сегодня, в условиях открытой информационной войны, как никогда требует пристального внимания к унификации подходов к законодательному регулированию и техническому обеспечению защиты информации о персональных данных своих граждан, а также защиты подрастающего поколения от информации, наносящей вред формированию сознания несовершеннолетних граждан.

Литература

1. Шейкин, А.Г. Информационная война [Электронный ресурс]. – URL: <http://www.council.gov.ru/services/discussions/blogs/136503/>.

2. Кихтан, В.В., Качмазова, З.Н. Информационная война: понятие, содержание и основные формы проявления // Вестник Волжского университета имени В.Н. Татищева, 2018. – № 2, том 2. – с. 228–234.

ЗАОЧНЫЕ ДОКЛАДЫ

УДК 054.056.53

О ПОДХОДЕ К ОЦЕНКЕ СТЕПЕНИ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОТ КИБЕРАТАК

О.К. БАРАНОВСКИЙ

*Открытое акционерное общество «АГАТ – системы управления» – управляющая компания
холдинга «Геоинформационные системы управления»,
г. Минск, Республика Беларусь*

В соответствии с Указом Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» (далее – Указ) одной из задач национальной системы обеспечения кибербезопасности является оценка эффективности защищенности объектов информационной инфраструктуры (далее – ОИИ) от кибератак. Центры обеспечения кибербезопасности и реагирования на киберинциденты (далее – центры кибербезопасности) будут проводить оценку степени защищенности ОИИ.

Ввиду фрагментарности глоссария в области кибербезопасности для понимания сущности процедуры оценки степени защищенности ОИИ следует обратиться к стандарту России ГОСТ Р 59709 [1], в котором, перефразируя в термины Указа, под оценкой степени защищенности от кибератак понимается процесс анализа возможности использования обнаруженных уязвимостей ОИИ для реализации кибератак.

При этом логичен вопрос: какой должна быть оценка – качественной или количественной, научно-обоснованной или субъектно-авторской, основанной на метрологии с повторяемостью результатов или в виде набора частных экспертных оценок.

Можно предположить, что порядок оценки степени защищенности ОИИ от кибератак будет регламентирован в виде требований к проведению набора проверок (аналог российского документа «Методические рекомендации по проведению мероприятий по оценке степени защищенности от компьютерных атак» с ограниченным доступом).

Будем считать, что оценка степени защищенности ОИИ должна осуществляться путем:

- анализа уязвимостей элементов (активов) ОИИ;
- контроля выполнения установленных требований по защите информации от кибератак;
- тестирования ОИИ на внешнее и внутреннее проникновение.

Для выполнения мероприятий необходима модель кибератак, учитывающая существующие и прогнозируемые возможности нарушителя на заданный период времени. Должно учитываться, что нарушитель может быть внешним, внутренним, а также совокупным по возможностям. Принятые меры защиты информации по отношению к внешнему нарушителю могут быть избыточными, а в то же время по отношению к внутреннему – недостаточными.

Результатом оценки степени защищенности ОИИ будут выявленные (почти всегда) уязвимые места в системе защиты информации (системе информационной безопасности), которые имеют место даже при выполнении установленных требований защиты информации.

В связи с этим следует ранжировать возможные состояния защищенности ОИИ, например, установить до шести степеней защищенности ОИИ от кибератак, полагая, что 1-я степень – максимальная, а 6-я – минимальная:

- 1-я степень – «полная защищенность»;
- 2-я степень – «высокая защищенность»;
- 3-я степень – «средняя защищенность»;
- 4-я степень – «удовлетворительная защищенность»;
- 5-я степень – «низкая защищенность»;
- 6-я степень – «неудовлетворительная защищенность».

Эффективность применения общей модели кибератак для конкретных ОИИ может быть повышена путем разработки частных моделей кибератак с учетом характеристик ОИИ и иных факторов. При этом всегда будут оставаться запроектные угрозы ввиду неполноты сведений об

уязвимостях ОИИ, используемых нарушителями техниках и инструментах, развитии информационных технологий. Поэтому присвоение степени «полная защищенность» ОИИ в результате оценки маловероятно.

Целесообразно ли использовать разные общие модели кибератак для ОИИ различной степени критичности (важности), в которых уровень технической и интеллектуальной оснащенности нарушителя варьируется, либо необходимо установить допустимую максимальную степень защищенности ОИИ в зависимости от степени его важности (критичности) – этот вопрос требует обсуждения.

К мероприятиям по оценке степени защищенности ОИИ, как правило, относят [2]:

- выявление уязвимостей сетевых служб и программного обеспечения (далее – ПО);
- контроль устранения ранее выявленных уязвимостей;
- контроль выполнения требований защиты информации, в том числе анализ настройки программных и программно-аппаратных средств ОИИ, средств защиты информации (далее – СрЗИ), анализ проектной, конструкторской и эксплуатационной документации;
- внешнее тестирование на проникновение;
- внутреннее тестирование на проникновение;
- тестирование устойчивости к атакам типа «отказ в обслуживании».

Соответственно, степень защищенности ОИИ от кибератак будет являться интегральной оценкой, формируемой из имеющих разный вес значимости частных показателей защищенности ОИИ от кибератак.

Следует учитывать, что такие наиболее важные проверки, как тестирование на проникновение, не могут быть проведены в должном объеме без риска нарушить безопасное функционирование ОИИ. В этом случае компенсирующей мерой будет использование киберполигона, состоящего из виртуальной инфраструктуры и физических объектов (сетевого и технологического оборудования, аппаратно-программных СрЗИ) и позволяющего моделировать конкретные ОИИ [3].

Тестирование на проникновение целесообразно осуществлять с использованием специального ПО, позволяющего реализовывать сценарии кибератак (последовательности определенных шагов), регистрируя факты обнаружения или необнаружения таких шагов средствами (механизмами) защиты информации. При этом, детализация сообщений от СрЗИ на разные действия (шаги) может значительно различаться – от простой записи событий информационной безопасности в журналы событий до сопоставления действий с определенной техникой из специализированной базы знаний, содержащей описание тактик, приемов и методов, используемых киберпреступниками, (например, Mitre Att&ck) с выдачей уведомления. В качестве метрик обычно используют процент обнаруженных несанкционированных воздействий на ОИИ.

Основными сложностями являются разработка полного набора сценариев кибератак по причине множества техник и способов их реализации и недостаток специалистов высокой компетенции, способных осуществить разработку и реализацию сценариев кибератак, аналогичных кибератакам в реальном мире.

Возможность вычисления оценки степени защищенности ОИИ от кибератак на основе измерения характеристик ОИИ (как при защите информации от утечки по техническим каналам) представляет собой труднореализуемую многопараметрическую задачу, зависящую не только от множества сценариев реализации кибератак, но и необходимости учета возможности их одновременного воздействия, а состояние защищенности ОИИ от кибератак динамически меняется с воздействиями на ОИИ и соответствующими им противодействиями со стороны системы защиты информации (системы информационной безопасности).

Возможно ли предложить методику оценки степени защищенности без проведения тестирования на проникновение на реальных ОИИ?

Задача оценки защищенности ОИИ в реальном времени может быть решена с применением подходов, использующих данные мониторинга поведения ОИИ в совокупности с ранее собранными данными больших объемов от различных субъектов.

Для анализа таких данных используются новые методы интеллектуальной обработки, в рамках которых формируются связи между «сырыми» данными, связанными с безопасностью, и высокоуровневыми метриками ОИИ, например, «защищенность ОИИ от кибератак», «киберустойчивость ОИИ» и т.п.

В частности, в [4] онтология кибербезопасности применяется для описания объекта как семантической модели метрик (метрики инфраструктуры, метрики атаки, метрики атакующего, метрики события, метрики реагирования и интегральные метрики) и данных, а использование динамически генерируемых данных о состоянии и поведении ОИИ в методике оценивания защищенности позволяет получать объективные оценки защищенности информационной системы от кибератак в реальном режиме времени. Авторы информируют о высоких затратах, связанных с повышением уровня детализации в целях построения наиболее полных моделей систем.

В связи с этим может быть использован математический аппарат нейронных сетей с применением методов глубокого обучения. Возможность применения нейронных сетей для различных типов задач кибербезопасности, таких, как обнаружение вторжений, обнаружение вредоносного ПО, анализ сетевого трафика, раскрытие утечек данных, выявление спама, описана в [5]. Использование онтологий позволяет оптимизировать и ускорить машинное обучение.

Таким образом, аппарат онтологий в кибербезопасности в совокупности с семантическим подходом позволяет выявлять скрытые уязвимости, оценивать возможность их использования для реализации кибератак, контролировать выполнение требований защиты информации. А использование аппарата нейронных сетей с глубоким обучением позволяет тестировать ОИИ на проникновение с минимальным риском нарушения функционирования ОИИ. Рассмотренные математические аппараты имеют высокий потенциал для автоматизации процедур оценки степени защищенности ОИИ центрами кибербезопасности.

Литература

1. ГОСТ Р 59709-2022. Защита информации. Управление компьютерными инцидентами. Термины и определения [Электронный ресурс]. – Режим доступа <https://files.stroyinf.ru/Data/792/79277.pdf>. – Дата доступа: 12.04.2023.
2. Опыт эксплуатации ГосСОПКА и необходимые технические компетенции [Электронный ресурс]. – Режим доступа: <https://www.itforumaltai.ru/upload/iblock/171/инфотекс.pdf>. – Дата доступа: 12.04.2023.
3. Сизоненко, А.Б. Методика экспериментальной оценки уровня защищенности информационных систем от компьютерных атак на базе киберполигона / А.Б. Сизоненко, И.С. Рудь, А.О. Титарев. // Электронный сетевой политематический журнал «Научные труды КубГТУ» [Электронный ресурс]. – 2022. – № 6. – С. 52–66. – Режим доступа: <https://ntk.kubstu.ru/data/mc/0092/4537.pdf>. – Дата доступа: 12.04.2023.
4. Дойникова, Е.В. Методика оценивания защищенности на основе семантической модели метрик и данных / Е.В. Дойникова [и др.] // Вопросы кибербезопасности. – 2021. – № 1 (41). – С. 29–40.
5. Гайфулина, Д.А. Применение методов глубокого обучения в задачах кибербезопасности. Часть 2. / Д.А. Гайфулина, И. В. Котенко // Вопросы кибербезопасности. – 2020. – № 4 (38). – С. 11–21.

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЕЯТЕЛЬНОСТИ ЦЕНТРОВ КИБЕРБЕЗОПАСНОСТИ

О.К. БАРАНОВСКИЙ, В.К. РЕЙШЕЛЬ

Открытое акционерное общество «АГАТ – системы управления» – управляющая компания холдинга «Геоинформационные системы управления», г. Минск, Республика Беларусь

Вступление в силу Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» (далее – Указ) создает условия для расширения рынка услуг по технической и криптографической защите информации в Беларуси в сфере кибербезопасности.

Следует ожидать, что до 14 августа 2023 года Оперативно-аналитический центр при Президенте Республики Беларусь (далее – ОАЦ) утвердит требования к центрам обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры (далее – центры кибербезопасности, SOC) и установит порядок проведения их аттестации.

Организации, закрепленные в Приложении 1 к Указу, и уполномоченные поставщики интернет-услуг, оказывающие услуги хостинга официальных интернет-сайтов и электронной почты, обеспечат создание в своей структуре центров кибербезопасности не позднее полутора лет со дня вступления в силу Указа, а определенные Советом Министров Республики Беларусь к 14 февраля 2024 года государственные органы и иные организации будут принимать решение о целесообразности создания и аттестации таких центров кибербезопасности в своей структуре либо приобретении услуг у организаций, их создавших.

Вместе с тем, на рынке услуг Республики Беларусь уже работают организации, имеющие лицензии и опыт по технической и криптографической защите информации, технические возможности которых могут обеспечивать кибербезопасность объектов информационной инфраструктуры (далее – ОИИ) иных субъектов.

Потенциальных участников рынка волнует вопрос: какие факторы окажут существенное влияние на выбор модели поведения на рынке услуг по обеспечению кибербезопасности, и как оказаться в лидерах?

Компания Kaspersky прогнозирует развитие трех моделей функционирования SOC [1]:

штатные SOC, функционирующие внутри организаций (с 2023 года будут создаваться в малом количестве ввиду существенных затрат);

SOC, оказывающие услуги владельцам ОИИ по модели Managed Security Service Provider (MSSP);

ведомственные SOC для государственных организаций и отраслей с высокой долей государственного участия (это приведет к появлению крупных проектов, в том числе по выстраиванию процессов не только внутри таких SOC, но и при взаимодействии с подчиненными организациями).

Можно предположить, что SOC, сформировавшие гибридную модель из ведомственных SOC и функционирующих по модели MSSP, имеют наилучший шанс для работы на рынках России и Беларуси.

Такие SOC, решив вопрос с материально-техническим обеспечением, будут набирать и обучать персонал, формировать базу знаний с необходимым информационно-аналитическим обеспечением своей деятельности.

ОАЦ, в соответствии с пунктом 7 Указа, примет необходимые меры по его реализации – будут определены требования по кибербезопасности ОИИ, установлены состав технических параметров киберинцидента, выработаны рекомендации по выявлению, предупреждению и исследованию кибератак, киберинцидентов, обеспечено их доведение до сведения центров кибербезопасности, определена типовая структура центров кибербезопасности и иные требования к ним.

Это позволит центрам кибербезопасности до начала их деятельности получить базовую методологию обеспечения кибербезопасности ОИИ, в том числе по сбору, обработке, анализу и обобщению информации о состоянии кибербезопасности на ОИИ, оценке степени защищенности ОИИ, установлению причин киберинцидентов, вызванных кибератаками на ОИИ.

При формировании нормативных и методических документов, можно предположить, будут использованы результаты научно-исследовательских и опытно-конструкторских работ, выполненных в рамках Программы Союзного государства «Совершенствование системы защиты информационных ресурсов Союзного государства и государств-участников Договора о создании Союзного государства в условиях нарастания угроз в информационной сфере (шифр «Паритет»)), утвержденной Постановлением Совета Министров Союзного государства от 11 июня 2018 года № 5, а именно:

- базовые модели угроз, атак и механизмы защиты ресурсов автоматизированных систем управления критически важных объектов (далее – АСУ КВО);
- перечень событий информационной безопасности (далее – ИБ) различных уровней автоматизированных систем управления технологическим процессом, включая АСУ КВО, необходимых для взаимодействия с СОС в рамках решения задач мониторинга ИБ;
- методики по обнаружению аномалий в сетевом потоке АСУ КВО;
- методики локализации, реагирования и предупреждения кибератак и киберинцидентов;
- рекомендации по устранению последствий киберинцидентов и координации мероприятий по устранению их последствий;
- методика оценки степени защищенности объектов критической инфраструктуры (далее – ОКИ) от кибератак;
- методика по установлению причин киберинцидентов, вызванных кибератаками на ОКИ.

Вместе с тем, для системной и непрерывной работы центров кибербезопасности, обеспечивающих кибербезопасность ОИИ в разных отраслях экономики, центры кибербезопасности будут вынуждены, опираясь на методическую помощь Национального центра кибербезопасности, создать собственные базы знаний, развивая их в рамках деятельности по обеспечению кибербезопасности.

Чтобы определить домены знаний (области) базы знаний информационно-аналитического обеспечения, необходимо рассмотреть, какие этапы деятельности по обеспечению кибербезопасности конкретных ОИИ требуют проведения аналитической работы:

- 1) подготовка стратегии обеспечения кибербезопасности:
 - сбор сведений об ОИИ (используемые информационные технологии, состав объектов, информационные потоки);
 - анализ (отбор) наиболее опасных уязвимостей;
 - оценка возможности реализации угроз ОИИ, оценка рисков кибератак и вызванных ими киберинцидентов по уровню ущерба;
 - оценка степени защищенности ОИИ с учетом выбранной частной модели угроз;
- 2) контроль (мониторинг) кибербезопасности ОИИ:
 - определение и постановка на мониторинг индикаторов компрометации объектов ОИИ, соответствующих им критичных событий ИБ согласно установленному составу технических параметров киберинцидента;
 - оценка степени защищенности ОИИ с учетом постановки на мониторинг кибератак и киберинцидентов;
- 3) обнаружение и реагирование на кибератаки и вызванные ими киберинциденты:
 - определение планов реагирования на кибератаки и вызванные ими киберинциденты;
 - локализация, реагирование и предупреждение кибератак и киберинцидентов;
 - оценка степени защищенности ОИИ с учетом реагирования на кибератаки и вызванные ими киберинциденты;
 - расследование (установление причин) кибератак и киберинцидентов;
 - устранение последствий кибератак и киберинцидентов.

В связи с этим необходимо сформировать облик информационно-аналитического обеспечения деятельности центров кибербезопасности. О формировании перспективных систем информационного обеспечения деятельности по защите информации от несанкционированного доступа (далее – НСД) указывалось в [2].

База знаний центра кибербезопасности должна содержать следующие домены знаний:

1. Сведения об ОИИ.

1.1. Состав системного и прикладного программного обеспечения (далее – ПО).

1.2. Состав средств вычислительной техники, сетевого и серверного оборудования.

1.3. Состав применяемых средств защиты информации.

1.4. Категории обрабатываемой информации.

1.5. Принадлежность, масштаб, топология и каналы связи с другими ОИИ.

2. Сведения об угрозах.

2.1. Сведения об угрозах НСД и сетевых атаках:

– источники угроз;

– способы реализации угроз (атак).

2.2. Сведения о свойствах (уязвимостях) ПО.

2.3. Сведения о вредоносном ПО.

2.4. Сведения о способах создания скрытых каналов передачи данных.

3. Сведения по видам обеспечения.

3.1. Нормативное обеспечение.

3.2. Методическое обеспечение:

– выявление и анализ уязвимостей;

– оценка возможности реализации (актуальности) угроз;

– оценка степени защищенности ОИИ и эффективности защиты информации;

– прогноз угроз НСД и сетевых атак;

– контроль защищенности ОИИ от кибератак;

– определение критичных событий ИБ в целях мониторинга кибербезопасности;

– локализация, реагирование и предупреждение кибератак и киберинцидентов;

– выбор планов защиты от кибератак;

– установление причин киберинцидентов, вызванных кибератаками;

– устранение последствий киберинцидентов, координация мероприятий по устранению их последствий.

3.3. Материально-техническое обеспечение.

3.4. Кадровое обеспечение.

3.5. Финансово-экономическое обеспечение.

4. Сведения, собранные в ходе осуществления деятельности.

4.1. Способы преодоления мер защиты при реализации кибератак на ОИИ.

4.2. Результаты оценки степени защищенности ОИИ.

4.3. Опыт применения мер и средств защиты информации от кибератак на ОИИ.

4.4. Новые технологии защиты информации от кибератак на ОИИ.

4.5. Результаты прогноза возникновения уязвимостей в системном и прикладном ПО, нового вредоносного ПО, новых способов кибератак на ОИИ.

Степень автоматизации непосредственно обнаружения и реагирования на кибератаки и киберинциденты зависит от наличия частных модели угроз НСД и сетевых атак, и сформированных на их основе моделей кибербезопасности конкретных ОИИ.

Однако, ввиду широкой номенклатуры используемых информационных технологий (а часто, и разработанного по заказу ПО), современные ОИИ настолько сложны, а внедрение мер и средств защиты информации имеет большую вариативность, поэтому аналитическими методами предсказать все последствия кибератак и киберинцидентов практически невозможно.

На состояние кибербезопасности существенно влияет человеческий фактор, когда, например, ответственные за обеспечение защиты информации на ОИИ держат в уме наличие «воздушного зазора» между корпоративной и технологической сетями ОИИ, а на практике

создают каналы связи для организации ограниченных информационных потоков, в том числе по управлению безопасностью сетей.

Накоплению знаний и формированию умений у персонала по обнаружению и реагированию на кибератаки и киберинциденты будет способствовать создание аппаратно-программной среды (киберполигона), в которой будут тренироваться как аналитики SOC, так и команды реагирования на киберинциденты.

Концептуально облик технологической части киберполигона зависит от выбранного метода моделирования ОИИ как сложной киберфизической системы [3].

Можно предположить, что номенклатура оказываемых услуг будет содержать следующие виды:

- сбор, обработка, анализ и обобщение информации о состоянии кибербезопасности на ОИИ, включая оценку степени защищенности ОИИ;
- выявление, предупреждение и исследование кибератак и вызванных ими киберинцидентов;
- реагирование на кибератаки и устранение последствий, вызванных ими киберинцидентов.

Степень полноты базы знаний информационно-аналитического обеспечения деятельности по обнаружению киберинцидентов и реагированию на кибератаки позволит сформировать пакеты услуг с разным уровнем обеспечения кибербезопасности (разной сложностью задач) ОИИ в зависимости от критичности таких объектов, и в перспективе, снизить среднюю цену услуг с ростом степени автоматизации процессов.

Соответственно, от этого будет зависеть рейтинг каждого центра кибербезопасности на рынке услуг.

Литература

1. Солдатов, С. Что ждет российские SOC в 2023 году [Электронный ресурс] / С. Солдатов, Р. Назаров. – Режим доступа: <https://securelist.ru/soc-socc-predictions-2023/106492/>. – Дата доступа: 07.04.2023.

2. Перспективы развития информационного обеспечения деятельности по защите информации в информационных системах союзного государства / Ю.К. Язов [и др.] // Комплексная защита информации: мат-лы XXVI науч.-практ. конф., Минск, 25–27 мая 2021 г. – С. 26–30.

3. Как мы построили виртуальную инфраструктуру для киберучений промышленных предприятий [Электронный ресурс] / О. Архангельский [и др.] – Режим доступа <https://habr.com/ru/companies/solarsecurity/articles/515626/>. – Дата доступа: 07.04.2023.

**ПОГЛОТИТЕЛИ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ
НА ОСНОВЕ ФОЛЬГИРОВАННЫХ МАТЕРИАЛОВ
ДЛЯ ЗАЩИТЫ СРЕДСТВ ОБРАБОТКИ ИНФОРМАЦИИ
ОТ ВОЗДЕЙСТВИЯ ПОМЕХ**

О.В. БОЙПРАВ, Н.В. БОГУШ, М.В. ПАВЛЕНКО, Е.С. БЕЛОУСОВА

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Защита средств обработки информации от воздействия помех является одним из мероприятий, реализуемых в целях обеспечения целостности и сохранности данных, обрабатываемых с помощью этих средств. Один их способов выполнения обозначенного мероприятия состоит в функциональном зонировании области помещения, в которой расположены средства вычислительной техники, с помощью мобильных перегородок, в конструкцию которых входят поглотители электромагнитного излучения. Такие поглотители характеризуются невысокой массой на единицу площади, что обуславливает устойчивость перегородок, в конструкцию которых они входят, а также невысокие ресурсозатраты на транспортировку последних [1, 2].

Авторами предложены новые поглотители электромагнитного излучения, перспективные для изготовления мобильных перегородок, предназначенных для функционального зонирования области помещения, в которой расположены средства вычислительной техники, в целях защиты этих средств от воздействия помех. Предложенные поглотители представляют собой нетканые волокнистые материалы, на одной из поверхностей которых закреплен лист фольгированного полимерного материала, а в объеме (между волокнами) которых с одинаковым шагом и периодичностью расположены макровключения сферической и полутороидальной форм, изготовленные на основе фольгированных материалов. Шаг расположения макровключений не превышает значения, равного половине длины электромагнитной волны на средней частоте рабочего диапазона частот поглотителя, а их размер сопоставим с этим значением [3, 4]. Макровключения полутороидальной формы ориентированы таким образом, что их плоскости ортогональны плоскостям волокнистых материалов, в которых они расположены.

Цель исследования, результаты которого представлены в докладе, состояла в установлении закономерностей изменения значений коэффициента поглощения электромагнитного излучения в диапазоне частот 2,0–17,0 ГГц, характерных для предложенных авторами поглотителей, в зависимости от шага, с которым в объеме последних расположены макровключения. Для достижения обозначенной цели были решены следующие задачи.

1. Выполнены измерения значений коэффициентов отражения и передачи электромагнитного излучения в диапазоне частот 2,0–17,0 ГГц предложенных поглотителей двух типов. У поглотителей типа 1 величина шага, с которым в их объеме были размещены макровключения, составляла 2,0 см (т.е. половину длины электромагнитной волны на средней частоте диапазона частот, в котором проводились измерения). У поглотителей типа 2 величина шага, с которым в их объеме были размещены макровключения, составляла 1,0 см.

2. На основе результатов выполненных измерений проведен расчет значений коэффициента поглощения электромагнитного излучения в диапазоне частот 2,0–17,0 ГГц предложенных поглотителей.

3. Выполнен сравнительный анализ рассчитанных значений, на основании результатов которого установлено, при каком шаге расположения макровключений в объеме предложенных поглотителей характерное для последних значения коэффициента поглощения электромагнитного излучения в диапазоне частот 2,0–17,0 ГГц является минимальным.

Диапазон частот, в котором проводились измерения, был выбран исходя из того, что ему принадлежат значения частот, характерные для электромагнитного излучения оборудования, используемого в настоящее время в промышленности и быту [5] и являющегося потенциальным источником помех для средств обработки информации.

На рисунке 1 представлены частотные характеристики коэффициента поглощения электромагнитного излучения предложенных поглотителей. Эти характеристики получены по результатам решения первой и второй задач в ходе достижения цели исследования.

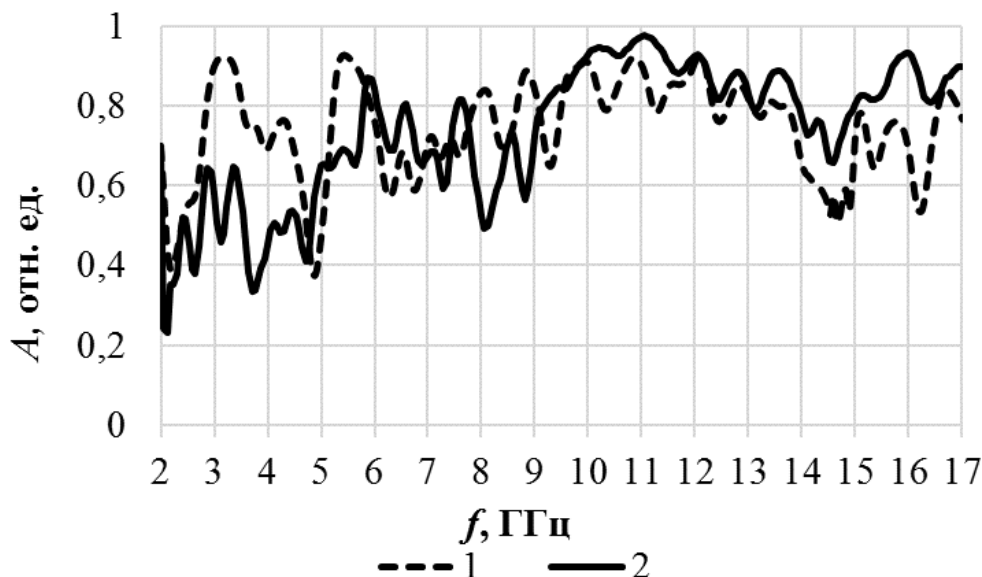


Рисунок 1. – Частотные зависимости коэффициента поглощения электромагнитного излучения в диапазоне частот 2,0–17,0 ГГц предложенных поглотителей типа 1 (кривая 1) и типа 2 (кривая 2)

Из рисунка 1 следует, что значения коэффициента поглощения электромагнитного излучения в диапазоне частот 5,0–17,0 ГГц предложенных поглотителей превышают 0,5, т.е. большая часть энергии взаимодействующего с этими поглотителями электромагнитного излучения в указанном диапазоне частот ослабляется ими за счет явления поглощения. Следует обратить внимание на то, что в диапазоне частот 9,5–14,0 ГГц значения указанного параметра изменяются в пределах от 0,8 до 0,95. Эта особенность обусловлена явлением рассеяния на макровключениях предложенных поглотителей электромагнитных волн, значение частоты которых принадлежит указанному диапазону частот. Предложенные и исследованные поглотители обеспечивают селективное поглощение энергии взаимодействующего с ними электромагнитного излучения в диапазоне частот 2,0–5,0 ГГц. При этом ширина полос поглощения электромагнитного излучения, характерных для поглотителей типа 1 (т.е. полос частот, в которых значения коэффициента поглощения электромагнитного излучения поглотителей более 0,5), превышает ширину аналогичных полос, характерных для поглотителей типа 2. Это обусловлено тем, что длина электромагнитных волн в диапазоне частот 2,0–5,0 ГГц превышает расстояние между шагом размещения макровключений в объеме поглотителей типа 2 и за счет этого такие волны в большей степени отражаются от макровключений, чем рассеиваются ими.

Таким образом, при изготовлении предложенных поглотителей представляется целесообразным располагать в их объеме макровключения с шагом, равным половине длины электромагнитной волны в рабочем диапазоне частот этих поглотителей. При соблюдении этой рекомендации можно обеспечить следующие преимущества для предложенных поглотителей по сравнению с поглотителями, в объеме которых макровключения должны быть расположены с шагом, величина которого менее половины длины волны на средней частоте рабочего их диапазона частот:

- пониженный расход фольгированных материалов для изготовления макровключений;
- пониженные временные на изготовление;
- более широкий диапазон частот (более широкие полосы частот), в котором (в которых) значения коэффициента поглощения электромагнитного излучения превышают 0,5.

Себестоимость предложенных поглотителей в 1,5–2,0 раза ниже себестоимости поглотителей, на основе которых изготавливаются экранирующие перегородки, представленные в [1, 2].

Литература

1. RF/EMI Shielded Curtains-Privacy and Separation! [Электронный ресурс]. – Режим доступа: <https://www.vtechtextiles.com/shielding/rf-emi-shielded-curtains-privacy-and-separation/>. – Дата доступа: 07.04.2023.
2. Large Faraday Tent – LX Black Shell RF/EMI Shielding Enclosure Room [Электронный ресурс]. – Режим доступа: <https://shop.faradaydefense.com/product/faraday-tents-rf-emi-shielding-enclosure-rooms/>. – Дата доступа: 07.04.2023.
3. Singh, A. Quad-Band FSS for Electromagnetic Shielding / A. Singh, C. Singh // International Journal of Computer Communication and Informatics, 2021. – Vol. 3, iss. 1. – P. 1–14.
4. Anwar, R.S. Frequency Selective Surfaces: A Review / R.S. Anwar, L. Mao, H. Ning // Applied Sciences, 2018. – Vol. 8, no. 9. 1689.
5. Shukla V. Review of electromagnetic interference shielding materials fabricated by iron ingredients. Nanoscale Advances, 2019. – № 5. – P. 1640–1671.

**ВОССТАНОВЛЕНИЕ АНАЛИТИЧЕСКОГО ЗАДАНИЯ
ПОРОГОВОЙ К-ЗНАЧНОЙ ФУНКЦИИ В УЗЛЕ ЗАЩИТЫ ИНФОРМАЦИИ
ПРИ НЕПОЛНЫХ ДАННЫХ**

А.В. БУРДЕЛЕВ

*Белорусский государственный университет,
г. Минск, Республика Беларусь*

Введение

Рассмотрим задачу восстановления аналитического задания функции усложнения $f(x_1, x_2, \dots, x_n)$ в узле защиты информации по известному входу и выходу. В случае применения пороговой к-значной функции в роли функции усложнения, задача нахождения ее аналитического задания может быть успешно решена по входу и выходу с помощью геометрического алгоритма характеристики к-значных пороговых функций, введенном в [1, 2].

1. Пороговые функции и их характеристика

Определение 1. [4] Функция к-значной логики $f(x_1, \dots, x_n)$, для которой существует линейная форма $L(x_1, \dots, x_n) = a_1x_1 + a_2x_2 + \dots + a_nx_n$, $x_i \in \mathbb{Z}_k$ с действительными коэффициентами и набор действительных порогов $b_0 < b_1 < \dots < b_k$ такие, что для всех $i \in \overline{0, k-1}$ выполняется условие

$$f(x_1, \dots, x_n) = i \Leftrightarrow b_i \leq L(x_1, \dots, x_n) < b_{i+1},$$

называется пороговой к-значной функцией. Не ограничивая общность определения, можем положить здесь и далее $b_0 = -\infty$ и $b_k = +\infty$. Пороговая к-значная функция может быть записана в следующем сокращенном виде: $f = [a_1, a_2, \dots, a_n; b_1, b_2, \dots, b_{k-1}]$.

Под алгоритмом характеристики пороговой к-значной функции, понимается процедура нахождения какого-либо семейства параллельных гиперплоскостей, разделяющих множества различных значений данной функции, то есть нахождения коэффициентов a_1, a_2, \dots, a_n линейной формы $L(x_1, \dots, x_n)$ и множества порогов b_0, b_1, \dots, b_{k+1} . Отметим, что характеристика имеет не единственное решение (например, все коэффициенты линейной формы и пороги могут быть домножены на ненулевой коэффициент); и вообще говоря каждой пороговой функции f можно поставить в соответствие класс \mathfrak{L}_f векторов коэффициентов и порогов, реализующих данную пороговую функцию:

$$\mathfrak{L}_f = \{(a_1, a_2, \dots, a_n, b_0, b_1, \dots, b_{k+1}) \mid f = [a_1, a_2, \dots, a_n; b_0, b_1, b_2, \dots, b_{k-1}]\}$$

В целом ряде разделов дискретной математики возникает задача распознавания принадлежности функции к некоторому классу и восстановления (характеристики) неизвестной дискретной функции из заданного класса с помощью последовательных вопросов о ее значениях в точках.

Определение 2. [1, 2, 3, 5] Для функции к-значной логики $f(x_1, \dots, x_n)$ коэффициентом роста по переменной x_i называется величина

$$\Delta_i = \sum_{(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \in \mathbb{Z}_k^{n-1}} (f(x_1, \dots, x_{i-1}, k-1, x_{i+1}, \dots, x_n) - f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n)).$$

Определение 3. [1, 2, 3, 5] Для функции к-значной логики $f(x_1, \dots, x_n)$ коэффициентом возрастания по переменной x_i называется величина

$$\lambda_i = \sum_{(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \in \mathbb{Z}_k^{n-1}} \sum_{l=0}^{k-2} \sum_{\varepsilon=l+1}^{k-1} (f(x_1, \dots, x_{i-1}, \varepsilon, x_{i+1}, \dots, x_n) - f(x_1, \dots, x_{i-1}, l, x_{i+1}, \dots, x_n)).$$

2. Геометрический алгоритм характеристики пороговых k -значных функций

В [1, 2] вводится геометрический алгоритм характеристики пороговых k -значных функций, а в [2] доказывается его сходимость на конечном шаге.

Условие 1. В силу неоднозначности задания пороговой функции будем полагать возможным использование порогов, удовлетворяющих нестрогому неравенству

$$b_0 \leq b_1 \leq \dots \leq b_k.$$

В случае равенства порогов $b_i = b_{i+1}$ для некоторого $i \in \overline{0, k-1}$, очевидно, функция $f(x_1, \dots, x_n)$ не принимает значения i . Также далее будем полагать строгое двухстороннее неравенство в определении пороговой k -значной функции:

$$f(x_1, \dots, x_n) = i \Leftrightarrow b_i < L(x_1, \dots, x_n) < b_{i+1}.$$

Этого всегда можно добиться небольшим изменением соответствующего порога или весов.

Определение 4. [1, 2] Будем говорить, что линейная форма $L(x_1, \dots, x_n) = a_1x_1 + a_2x_2 + \dots + a_nx_n$ дает чистое разделение областей значений пороговой k -значной функции $f(x_1, \dots, x_n)$, принимающей все значения из множества \mathbb{Z}_k , если для любого $\alpha \in \overline{0, k-2}$ выполняется строгое неравенство

$$\max_{f(\varepsilon_1, \dots, \varepsilon_n) = \alpha} \{a_1\varepsilon_1 + \dots + a_n\varepsilon_n\} < \min_{f(\varepsilon_1, \dots, \varepsilon_n) = \alpha+1} \{a_1\varepsilon_1 + \dots + a_n\varepsilon_n\}$$

Если это выполняется, то границы b_0, b_1, \dots, b_k можно определить, например, следующим способом:

$$b_\alpha = \min_{f(\varepsilon_1, \dots, \varepsilon_n) = \alpha} \{a_1\varepsilon_1 + \dots + a_n\varepsilon_n\}, \alpha \in \overline{0, k-1},$$

$$b_k = \max_{f(\varepsilon_1, \dots, \varepsilon_n) = k-1} \{a_1\varepsilon_1 + \dots + a_n\varepsilon_n\} + 1.$$

В случае, когда функция $f(x_1, \dots, x_n)$ не принимает некоторых значений из множества $\overline{0, k-1}$, необходимо следующим образом убрать из рассмотрения соответствующие области значений: пусть функция $f(x_1, \dots, x_n)$ принимает значения $0 \leq \alpha_0 < \alpha_1 < \dots < \alpha_t < k$, $0 < t < k$. Тогда для всех $i \in \overline{0, t-1}$ необходимо проверить выполнение строгого неравенства

$$\max_{f(\varepsilon_1, \dots, \varepsilon_n) = \alpha_i} \{a_1\varepsilon_1 + \dots + a_n\varepsilon_n\} < \min_{f(\varepsilon_1, \dots, \varepsilon_n) = \alpha_{i+1}} \{a_1\varepsilon_1 + \dots + a_n\varepsilon_n\}.$$

Пороги в этом случае можно определить, например, по правилу: для всех значений $\alpha_0, \dots, \alpha_t$ присвоить значения

$$b_{\alpha_i} = \min_{f(\varepsilon_1, \dots, \varepsilon_n) = \alpha_i} \{a_1\varepsilon_1 + \dots + a_n\varepsilon_n\};$$

далее, если функция принимает значение $k-1$, то положить

$$b_k = \max_{f(\varepsilon_1, \dots, \varepsilon_n) = k-1} \{a_1\varepsilon_1 + \dots + a_n\varepsilon_n\} + 1,$$

в противном случае положить $b_k = +\infty$; для оставшихся значений $j \in \mathbb{Z}_k \setminus \{\alpha_0, \dots, \alpha_t\}$ (которые не являются значениями функции $f(x_1, \dots, x_n)$) начиная со старшего присвоить соответствующему порогу значение $b_j = b_{j+1}$.

Обозначим далее для всех $i = \overline{0, k-1}$:

$$F_i = \{(x_1, \dots, x_n) \in \mathbb{Z}_k^n \mid f(x_1, \dots, x_n) = i\},$$

$$\max(F_i) = \max_{(x_1, \dots, x_n) \in F_i} \{L(x_1, \dots, x_n)\},$$

$$x_{\max}(F_i) = \{(x_1, \dots, x_n) \in \mathbb{Z}_k^n \mid L(x_1, \dots, x_n) = \max(F_i)\},$$

$$\min(F_i) = \min_{(x_1, \dots, x_n) \in F_i} \{L(x_1, \dots, x_n)\},$$

$$x_{\min}(F_i) = \{(x_1, \dots, x_n) \in \mathbb{Z}_k^n \mid L(x_1, \dots, x_n) = \min(F_i)\}.$$

В случае если $F_i = \emptyset$, положим $\max(F_i) = +\infty$, $\min(F_i) = -\infty$, $x_{\max}(F_i) = (-1, \dots, -1)$ и $x_{\min}(F_i) = (-1, \dots, -1)$.

Геометрический алгоритм характеристики пороговых k -значных функций

Вход алгоритма: вектор значений функции $f(x_1, \dots, x_n)$.

Пусть пороговая функция $f(x_1, \dots, x_n)$ принимает только значения $0 \leq \alpha_0 < \alpha_1 < \dots < \alpha_t < k$, $0 < t < k$.

1. Инициализация

Проинициализировать начальный вектор коэффициентов линейной формы коэффициентами роста либо коэффициентами возрастания:

$$(a_1, \dots, a_n) := (\Delta_1, \Delta_2, \dots, \Delta_n) \text{ либо } (a_1, \dots, a_n) := (\lambda_1, \lambda_2, \dots, \lambda_n).$$

2. Вычисление проверочной таблицы

Для всех $i = \overline{0, t}$, вычислить $\min(F_{\alpha_i})$, $\max(F_{\alpha_i})$.

3. Проверка чистого разделения областей значений функции

Для каждого $i = \overline{0, t-1}$ проверить выполнение неравенства

$$\max(F_{\alpha_i}) \geq \min(F_{\alpha_{i+1}}).$$

В случае выполнения неравенства для некоторого $i \in \{0, \dots, t-1\}$ перейти к блоку «Коррекция» с параметрами (α_i, α_{i+1}) . В противном случае перейти к блоку «Вычисление порогов».

Блок «Коррекция». Входным параметром блока является пара (α_i, α_{i+1}) .

4. Выбор точек

Произвольным образом выбрать точки $(x_1, \dots, x_n) \in x_{\max}(F_{\alpha_i})$ и $(y_1, \dots, y_n) \in x_{\min}(F_{\alpha_{i+1}})$

5. Коррекция линейной формы

Для всех $j \in \overline{1, n}$ присвоить $a_j = a_j - x_j + y_j$.

6. Возврат в основной цикл

Вернуться в пункт 2 основного алгоритма

Блок «Вычисление порогов»

Для всех значений $\alpha_0, \dots, \alpha_t$ присвоить значения

$$b_{\alpha_i} = \min_{f(\varepsilon_1, \dots, \varepsilon_n) = \alpha_i} \{a_1 \varepsilon_1 + \dots + a_n \varepsilon_n\}.$$

Если функция принимает значение $k-1$, то положить

$$b_k = \max_{f(\varepsilon_1, \dots, \varepsilon_n) = k-1} \{a_1 \varepsilon_1 + \dots + a_n \varepsilon_n\} + 1,$$

в противном случае положить $b_k = +\infty$; для оставшихся значений $j \in \mathbb{Z}_k \setminus \{\alpha_0, \dots, \alpha_t\}$ (которые не являются значениями функции $f(x_1, \dots, x_n)$) начиная со старшего присвоить соответствующему порогу значение $b_j = b_{j+1}$.

Выход алгоритма: векторы (a_1, \dots, a_n) , (b_0, \dots, b_k) .

3. Восстановление аналитического задания пороговой k -значной функции в узле защиты информации при неполных данных

Как правило при решении задачи восстановления аналитического задания функции усложнения $f(x_1, x_2, \dots, x_n)$ по известному входу и выходу в распоряжении имеются значения функции $f(x_1, x_2, \dots, x_n)$ не во всех точках. В этом случае на задачу характеристики пороговой функции накладываются дополнительные ограничения – неполные данные.

Определение 5. Функцию $f(x_1, \dots, x_n): M \rightarrow \mathbb{Z}_k$, где $M \subseteq \mathbb{Z}_k^n$, для которой существует линейная форма $L(x_1, \dots, x_n) = a_1 x_1 + a_2 x_2 + \dots + a_n x_n, x_i \in \mathbb{Z}_k$ с действительными коэффициентами и набор действительных порогов $b_0 < b_1 < \dots < b_k$ такие, что для всех $i \in \overline{0, k-1}$ выполняется условие

$$f(x_1, \dots, x_n) = i \Leftrightarrow b_i \leq L(x_1, \dots, x_n) < b_{i+1},$$

будем называть частично известной пороговой k -значной функцией. Не ограничивая общность определения, можем положить здесь и далее $b_0 = -\infty$ и $b_k = +\infty$.

Под алгоритмом характеристики частично известной пороговой k -значной функции, понимается процедура нахождения какого-либо семейства параллельных гиперплоскостей, разделяющих множества различных значений данной функции, то есть нахождения коэффициентов a_1, a_2, \dots, a_n линейной формы $L(x_1, \dots, x_n)$ и множества порогов b_0, b_1, \dots, b_{k+1} .

Рассмотрим применение геометрического алгоритма для характеристики частично известной пороговой k -значной функции. Для этого следует определиться как действовать геометрическому алгоритму в случае, когда он обращается к точке, в которой значение искомой функции неизвестно, то есть в терминах Определения 5 обращается к точке из множества $\mathbb{Z}_k \setminus M$. Геометрический алгоритм обращается к значениям функции в следующих двух случаях:

1. При подсчете коэффициентов роста либо коэффициентов возрастания для первичной аппроксимации линейной формы.

2. При вычислении максимумов и минимумов значений линейной формы в областях значений искомой функции.

Наиболее простым и логичным действием при отсутствии информации о значении функции в точке видится игнорирование данной точки, которое в обоих случаях должно быть реализовано следующим образом:

1. При подсчете коэффициентов роста либо коэффициентов возрастания в соответствующих им суммах

$$\Delta_i = \sum_{(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \in \mathbb{Z}_k^{n-1}} (f(x_1, \dots, x_{i-1}, k-1, x_{i+1}, \dots, x_n) - f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n)),$$

$$\lambda_i = \sum_{(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \in \mathbb{Z}_k^{n-1}} \sum_{l=0}^{k-2} \sum_{\varepsilon=l+1}^{k-1} (f(x_1, \dots, x_{i-1}, \varepsilon, x_{i+1}, \dots, x_n) - f(x_1, \dots, x_{i-1}, l, x_{i+1}, \dots, x_n))$$

игнорируются слагаемые, для вычисления которых осуществляется обращение к неизвестному значению искомой функции.

2. При вычислении максимума $\max(F_{\alpha_i})$ и минимума $\min(F_{\alpha_i})$ значений линейной формы в областях значений искомой функции следует игнорировать значение линейной формы в данной точке.

Определение 6. Будем называть геометрический алгоритм для характеристики пороговой k -значной функции, обрабатывающий точки из множества $\mathbb{Z}_k \setminus M$ указанным выше способом, геометрическим алгоритмом для характеристики частично известной пороговой k -значной функции.

Рассмотрим, применение геометрического алгоритма для характеристики пороговой функции при неполных данных. Актуальным вопросом является сходимость данного алгоритма. Для доказательства сходимости необходимо рассмотреть вопрос принадлежности к одному ортанту коэффициентов роста и возрастания и вектора коэффициентов линейной формы частично известной пороговой k -значной функции.

Теорема 1. Пусть частично известная пороговая k -значная функция $f(x_1, \dots, x_n)$, задается линейной формой

$$L(x_1, \dots, x_n) = a_1x_1 + a_2x_2 + \dots + a_nx_n.$$

Обозначим вектор $\vec{L} = (a_1, a_2, \dots, a_n)$. Тогда вектор коэффициентов роста $(\Delta_1, \Delta_2, \dots, \Delta_n)$ и вектор коэффициентов возрастания $(\lambda_1, \lambda_2, \dots, \lambda_n)$ лежат в одном ортанте с вектором \vec{L} либо некоторые их координаты равны нулю. Другими словами, знаки соответствующих координат у всех трех векторов совпадают с точностью до равенства нулю.

Теорема 2. Если $f(x_1, \dots, x_n)$ – частично известная пороговая k -значная функция, то геометрический алгоритм характеристики частично известной пороговой k -значной функции сходится за конечное число шагов и дает ее реализацию.

Заключение

Таким образом, задача восстановления аналитического задания пороговой функции усложнения при неполных данных может быть успешно решена с помощью геометрического алгоритма характеристики частично известной пороговой k -значной функции. При этом будет построена некоторая пороговая функция, которая будет совпадать с частично известной пороговой k -значной функцией во всех точках множества M .

Список литературы

1. Бурделев А.В., Никонов В.Г. О новом алгоритме характеристики k значных пороговых функций // Computational nanotechnology, Выпуск № 1, 2017. – С. 7–14.
2. Бурделев А.В. О сходимости нового алгоритма характеристики k -значных пороговых функций // Прикладная дискретная математика, 2018. – № 39. – С. 107–115.
3. Никонов В. Г., Никонов Н. В. Особенности пороговых представлений k значных функций // «Труды по дискретной математике», 2008. – Т. 11. – с. 60–85.
4. Бурделев А.В., Никонов В.Г. О построении аналитического задания k -значной пороговой функции // Computational nanotechnology, Выпуск № 2, 2015. – С. 5–13.

ОПРЕДЕЛЕНИЕ ОПТИМАЛЬНОГО МАРШРУТА ДЛЯ ПРОКЛАДКИ VPN-ТУННЕЛЕЙ ПО КОМПЛЕКСНОЙ МЕТРИКЕ В СЕТИ ЭЛЕКТРОСВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

С.С. ВРУБЛЕВСКИЙ, А.А. БЫСОВ

*Учреждение образования «Военная академия Республики Беларусь»
Минск, Республика Беларусь*

На сегодня исследование *Virtual Private Network (VPN)* направлены на совершенствования их основных сетевых характеристик в глобальных сетях, в которых *Quality of Service* обеспечивается путем расширения пропускной способности, что не является допустимым в сети электросвязи специального назначения (СЭСН) с низкоскоростными участками, использующими технологию коммутации каналов [1].

Наличие эффекта «бутылочного горлышка» и учет в качестве ресурса сети только пропускной способности, приводит не только к снижению показателей *QoS* в *VPN*-туннеле [2], но и к ошибочному определению ресурса сети для их прокладки [3]. Следовательно, для определения оптимального маршрута для прокладки *VPN*-туннелей в СЭСН, необходимо применять методы, учитывающие в качестве ресурса сети не только полосу пропускания канала связи, но и задержку передачи пакета.

Транспортную сеть СЭСН можно описать с помощью теории графов, где X – количество вершин графа (маршрутизаторов), A – количество ребер (соединительных линий между маршрутизаторами). В связи с учетом не только пропускной способности, но и задержки передачи пакета при поиске оптимального маршрута для прокладки *VPN*-туннеля, предлагается использовать для обозначения ребра комплексную метрику – два веса: полосу пропускания C_{ij} и суммарную задержку передачи пакета между вершинами i и j на ребре $w_{ij}^{(h)}$.

Следует отметить, что к каждому *VPN*-туннелю предъявляются требования по пропускной способности и задержки передачи пакета для определенного класса трафика, тогда создание *VPN*-туннелей сопровождается уменьшением ресурса сети, что приводит к сокращению запаса по пропускной способности на каждом ребре двухвесового графа.

Запас ребра по пропускной способности определяется как

$$\Delta_e^{(h)} = q_e - \lambda_e^{(h-1)}, \quad (1)$$

где q_e – пропускная способность ребра e ; $\lambda_e^{(h-1)}$ – интенсивность трафика на ребре e , на предыдущем шаге $h-1$ перед созданием *VPN*-туннеля; E – множество ребер e , входящих в оптимальный маршрут для прокладки *VPN*-туннеля h .

При решении задачи поиска оптимального маршрута для прокладки *VPN*-туннеля необходимо найти маршрут с минимальной задержкой передачи пакета, меньшей либо равной пороговому значению задержки передачи пакета для определенного класса трафика k , и с максимальным запасом по пропускной способности на ребре e , что определяет следующую целевую функцию

$$\sum_{h=1}^H \sum_{e=1}^E \frac{w_e^{(h)}}{\Delta_e^{(h)}} = \sum_{h=1}^H \sum_{e=1}^E \frac{w_e^{(h)}}{q_e - \lambda_e^{(h-1)}} \rightarrow \min, \quad (2)$$

с ограничением

$$\sum_{e=1}^E w_e^{(h)} \leq w_{\text{доп } k}^{(h)}, \quad \forall k, \quad (3)$$

где H – множество создаваемых VPN-туннелей; $\sum_{e=1}^E w_e^{(h)}$ – суммарная задержка передачи пакета всего оптимального маршрута, состоящего из ребер e из множества E для планируемого VPN-туннеля h ; $\frac{w_e^{(h)}}{q_e - \lambda_e^{(h-1)}}$ – удельный запас по пропускной способности на ребре e , являющейся метрикой для решения задачи оптимальной организации VPN-туннелей; $w_{\text{доп } k}$ – максимально допустимая задержка передачи для пакетов k -ого класса ($k = \overline{1, 7}$) в соответствии с [4].

Целевая функция (2) нелинейная, а ограничение (3) представлено в форме нелинейного неравенства.

Для решения задачи (2) необходимы следующие исходные данные: матрица пропускных способностей в сети между маршрутизаторами i и j – $\mathbf{Q} = [q_e]$; матрица суммарной задержки передачи пакета между маршрутизаторами i и j – $\mathbf{W}^{(h)} = [w_e^{(h)}]$; матрица интенсивности трафика, циркулирующего между маршрутизатором i и j $\mathbf{\Lambda}_e^{(h-1)} = [\lambda_e^{(h-1)}]$; матрица удельных запасов по пропускной способности между маршрутизатором i и j $\mathbf{\Phi} = [\varphi_e]$; i_h – номер маршрутизатора, от которого прокладывается VPN-туннель (исток); s_h – номер маршрутизатора к которому прокладывается VPN-туннель (сток); q_h – интенсивность трафика в создаваемом VPN-туннеле; $w_{\text{доп } k}$ – максимально допустимая задержка передачи пакетов в структуре VPN-туннеля в соответствии с классом трафика.

Совокупность векторов, каждый из которых представляет собой набор узлов, характеризующий их последовательное соединение в оптимальном маршруте для прокладки VPN-туннеля имеет следующий вид

$$\left\{ \begin{array}{l} \text{VPN}_1 = \{i_1, j_{11}, j_{12}, \dots, j_{1f}, s_1\}, \\ \text{VPN}_2 = \{i_2, j_{21}, j_{22}, \dots, j_{2f}, s_2\}, \\ \dots \\ \text{VPN}_h = \{i_h, j_{h1}, j_{h2}, \dots, j_{hf}, s_h\}. \end{array} \right. \quad (4)$$

В соответствии с (1), (5), (6), (4) целевая функция (2) определяется как

$$\left\{ \begin{array}{l} \sum_{h=1}^H \sum_{e=1}^E \frac{w_e^{(1)}}{\Delta_e^{(1)}} = \frac{w_{i_1 j_{11}}^{(1)}}{q_{i_1 j_{11}} - \lambda_{i_1 j_{11}}^{(0)}} + \frac{w_{j_{11} j_{12}}^{(1)}}{q_{j_{11} j_{12}} - \lambda_{j_{11} j_{12}}^{(0)}} + \dots + \frac{w_{1 f s_1}^{(1)}}{q_{1 f s_1} - \lambda_{1 f s_1}^{(0)}}, \\ \sum_{h=1}^H \sum_{e=1}^E \frac{w_e^{(2)}}{\Delta_e^{(2)}} = \frac{w_{i_2 j_{21}}^{(1)}}{q_{i_2 j_{21}} - \lambda_{i_2 j_{21}}^{(1)}} + \frac{w_{j_{21} j_{22}}^{(1)}}{q_{j_{21} j_{22}} - \lambda_{j_{21} j_{22}}^{(1)}} + \dots + \frac{w_{2 f s_2}^{(1)}}{q_{2 f s_2} - \lambda_{2 f s_2}^{(1)}}, \\ \dots \\ \sum_{h=1}^H \sum_{e=1}^E \frac{w_e^{(h)}}{\Delta_e^{(h)}} = \frac{w_{i_2 j_{21}}^{(h)}}{q_{i_2 j_{21}} - \lambda_{i_2 j_{21}}^{(h)}} + \frac{w_{j_{21} j_{22}}^{(h)}}{q_{j_{21} j_{22}} - \lambda_{j_{21} j_{22}}^{(h)}} + \dots + \frac{w_{2 f s_2}^{(h)}}{q_{2 f s_2} - \lambda_{2 f s_2}^{(h)}}. \end{array} \right. \quad (5)$$

Ограничение (3) с учетом (4) примет следующий вид

$$\begin{cases} w_{i_1 j_{11}}^{(1)} + w_{j_{11} j_{12}}^{(1)} + \dots + w_{1 f s_1}^{(1)} \leq w_{\text{доп } k}^{(1)}, \\ w_{i_2 j_{21}}^{(2)} + w_{j_{21} j_{22}}^{(2)} + \dots + w_{2 f s_2}^{(2)} \leq w_{\text{доп } k}^{(2)}, \\ \dots \\ w_{i_h j_{h1}}^{(h)} + w_{j_{h1} j_{h2}}^{(h)} + \dots + w_{h f s_h}^{(h)} \leq w_{\text{доп } k}^{(h)}. \end{cases} \quad (6)$$

На каждом шаге необходимо определить путь для одного VPN-туннеля, т.е. определять минимум функции (5), после чего пересчитывать матрицу задержки передачи пакетов (6), далее выполнить вычисления повторно. С учетом нелинейного вида функции (5) и итеративного подхода в поиске оптимальных маршрутов для создаваемых VPN-туннелей применен аппарат тропической математики.

Применение аппарата тропической математики осуществляется заменой арифметических операций (сложение, умножение) другим набором операций (такими как максимум (минимум)), при этом происходит замена числовых полей тропическими полукольцами и полуполями. Для решения задачи минимизации (5) вводится матрица Φ^* , являющейся также матрицей наименьших расстояний, которая определяется как

$$\Phi^* = \bigoplus_{x=1}^{X-1} \Phi^x = I \oplus \Phi \oplus \Phi^2 \oplus \dots \oplus \Phi^{X-1},$$

где I – единичная матрица, определенная в тропическом полукольце.

Определение элементов матрицы Φ^* производится путем возведения матрицы Φ в степень $X - 1$ в тропическом полукольце, а элементы матрицы Φ^* определяются как $\Phi^* = [\varphi_{xx}^*]$, где $\varphi_{xx}^* = \min\{I, \min\{\varphi_{x1} + \varphi_{1x}, \varphi_{x2} + \varphi_{2x}, \dots, \varphi_{xx} + \varphi_{xx}\}\}$ – удельный запас по пропускной способности (наименьшее расстояние) между любыми двумя маршрутизаторами, после тропического возведения матрицы Φ в степень $X - 1$.

Имея матрицу наименьших расстояний между любыми двумя маршрутизаторами, можно восстановить оптимальный маршрут для прокладки VPN-туннелей. Для этого необходимо выбрать начальную и конечную точку между которыми планируется VPN-туннель – i_h и s_h , далее найти число

$$\Theta = \bigoplus (\varphi_{i_h g} \otimes \varphi_{g s_h}^*) = \bigoplus \min\{\varphi_{i_h g_1} + \varphi_{g_1 s_h}^*, \varphi_{i_h g_2} + \varphi_{g_2 s_h}^*, \dots, \varphi_{i_h g} + \varphi_{g s_h}^*\}, \quad (7)$$

где g – узел смежный узлу i_h .

Узел g добавляем в вектор VPN_h только при выполнении равенств: $\Theta = \varphi_{i_h g} + \varphi_{g s_h}^*$ и $i_h = g$. После этого производится повтор вычисления (7), до тех пор, пока $g \neq s_h$.

Для оценки эффективности предлагаемого метода определения оптимального маршрута для планируемого VPN-туннеля, при сравнении со способами определения оптимального маршрута без учета задержки передачи пакета, а именно *RIP* и *OSPF*, было проведено исследование на типовой структуре СЭСН [5]. В результате которого были получены зависимости, представленные на рисунке 1.

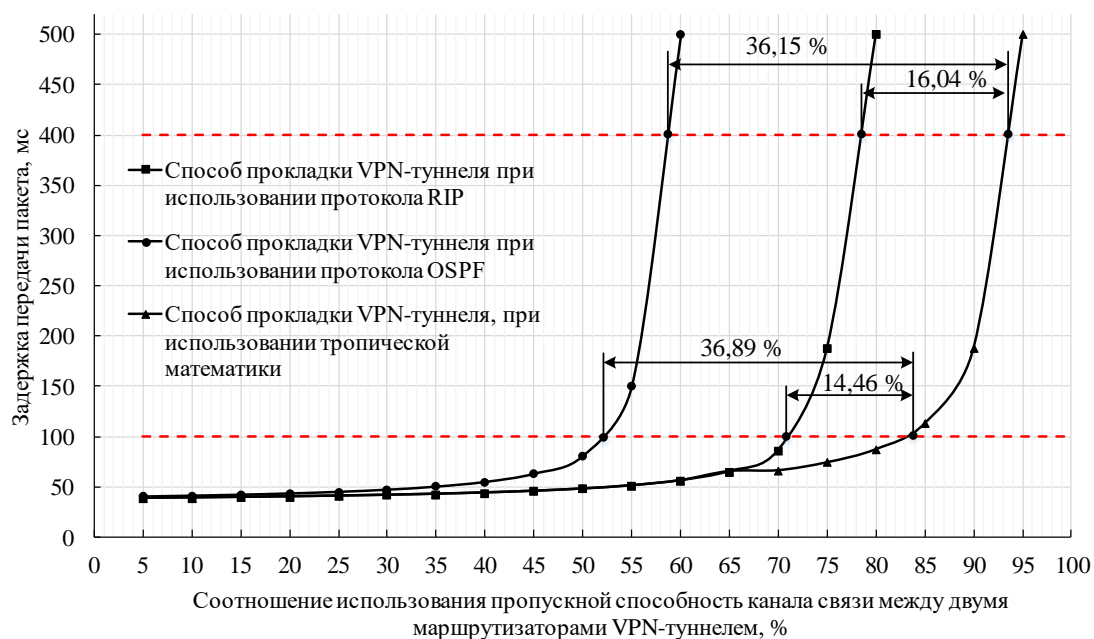


Рисунок 1. – Зависимости задержки передачи пакета от интенсивности трафика для различных способов прокладки VPN-туннеля

Данные зависимости являются средним значением данных, полученных при измерении в 150 вариантах организации VPN-туннеля между точками, находящимися в различных местах сети. (между маршрутизаторами, находящимися в ядре сети, на значительном удалении от ядра сети, и т.д.).

Таким образом, определен метод параметрического синтеза сети VPN, отличающийся учетом задержки передачи пакета и позволяющий при помощи математического аппарата тропической математики достигнуть значение задержки передачи пакета в 100 мс, для протокола OSPF, при 52 % использовании VPN-туннелем пропускной способности канала связи, для RIP – 71 %, а для предлагаемого способа прокладки VPN-туннелей при 83 %.

Литература

1. Лукьянчик, В.Н. Современные и перспективные информационные и телекоммуникационные технологии на сетях связи специального назначения / В.Н. Лукьянчик, А.В. Селезнев, В.Н. Мельник [и др.] // Труды ЦНИСС. Санкт-Петербургский филиал. – 2022. – Т. 1, № 13. – С. 52–57.
2. Машкин, Е.В. Анализ характеристик качества обслуживания сети VPN на основе имитационной модели / Е.В. Машкин, А.А. Бысов, С.С. Врублевский // Весн. сувязі. – 2022. – № 5 (175). – С. 68–72.
3. Врублевский, С.С. Обоснование необходимости учета задержки передачи пакетов при планировании VPN-туннелей в сетях электросвязи специального назначения / С.С. Врублевский, Е.В. Машкин, А.А. Бысов // Вестник ВАРБ – 2023. – № 1 (78). – С. 24–31
4. Требования к сетевым показателям качества для служб, основанных на протоколе IP: Рекомендация Y.1541. – Женева: МСЭ, 2006. – 16 с.
5. Разработать и организовать производство аппаратно-программного комплекса средств коммутации и маршрутизации цифровых потоков для полевых систем связи: отчет об ОКР / ОАО «АГАТ-СИСТЕМ»; рук. В.М. Зайцев. – 2009. – 124 с.

ПРИМЕНЕНИЕ МЕТОДОВ ОПТИМИЗАЦИИ НА РАЗНЫХ СТАДИЯХ СОЗДАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

В. ДИЧЕНКОВА

*Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»,
г. Санкт-Петербург, Российская Федерация*

Введение

В соответствии с ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» создание системы защиты информации (СЗИ) подразделяется на пять этапов:

- формирование требований к системе защиты информации (ЗИ) автоматизированной системы защиты информации (АСЗИ);
- разработка (проектирование) системы ЗИ АСЗИ;
- внедрение системы ЗИ АСЗИ;
- аттестация АСЗИ на соответствие требованиям безопасности информации и ввод ее в действие;
- сопровождение системы ЗИ в ходе эксплуатации АСЗИ.

Обзор проводится в целях определения принципов, методов или алгоритмов, подходящих для формирования методики выбора мер защиты информации. Этот шаг относится к третьему этапу создания СЗИ, однако будут рассмотрены и методы, используемые на других этапах. Использование математических методов позволяет оптимизировать процесс принятия решений, сделать его более объективным, автоматизированным и наглядным. Таким образом, актуальность применения методов оптимизации в процессе создания СЗИ складывается из постоянной необходимости обеспечить обоснованный и объективный выбор лицами, принимающим решения.

1. Постановка задачи

Задачи по разработке СЗИ на всех этапах так или иначе решаются в том числе посредством выбора наиболее предпочтительного варианта в конечных множествах.

В рассматриваемых работах используются различные варианты автоматизированных средств формального синтеза совместно со средствами анализа и оценки характеристик создаваемого объекта, и поддержки принятия решений в интерактивном режиме.

Задача по оптимальному выбору мер защиты информации включает в себя ряд основных подзадач:

- предложение множества оцениваемых вариантов (альтернатив) в наглядной и удобной форме (x – множество альтернатив, D – множество допустимых значений x);
- определение значений показателей и критериев оптимальности ($f(x)$ – целевая функция, математически выражающая критерии оптимальности);
- установление ограничений на множество допустимых значений альтернатив ($w(x), z(x)$);
- формирование предпочтений в условиях многокритериальной оптимизации;
- выбор методов поиска оптимальных вариантов;
- решение задачи оптимизации.

В общем виде задачу можно представить следующим образом:

$$\begin{aligned} f(x) &\rightarrow \text{extr}, \\ x &\in D, \\ w(x) &> n, z(x) \leq m. \end{aligned} \tag{1}$$

В качестве входных значений для методики выбраны возможные меры защиты информации, объединенные в наборы по таким признакам, как принципы реализации, ранжирование по уровню покрываемого риска, необходимость выполнения требований законодательства и другие, набор критериев (например, время реализации и затрачиваемые ресурсы) и ограничений.

Также необходимо учесть, что многие требования и показатели носят качественный характер, из чего неизбежно следует присутствие человека как в процессе постановки задачи, так и при ее решении.

2. Обзор применяемых методов оптимизации

2.1 Балльные оценки

Так, в работе [1] была предложена методика выбора структуры СЗИ на основе балльных экспертных оценок в шкале от пяти показателей. В качестве показателей оценок были использованы:

- надежность;
- быстродействие;
- прозрачность для пользователя;
- глобальность;
- стоимость.

При этом остается субъективность оценок, зависящая от привлекаемых экспертов. Предложенная функция выглядит следующим образом:

$$I_3 = \sum_{i=1}^n (I_{max} - I_i)^2, \quad (2)$$

где n – количество показателей,

I_i – оценка i -го показателя,

I_{max} – максимальное значение шкалы оценок.

2.2 Линейное программирование

В работе [2] линейное программирование используется для выбора инструментального средства для разработки СрЗИ, которое можно отнести к этапу проектирования СЗИ.

$$E = \varphi(q) = \varphi(q_1, q_2, \dots, q_n) \quad (3)$$

$$E = \varphi(q) = \varphi(q_1, q_2, \dots, q_n) = \sum_{i=1}^n b_i q_i \quad (4)$$

Значения коэффициента b_i отражают полезность (ценность) показателя q_i при принятии сложного решения о выборе альтернативы.

В качестве программного обеспечения для реализации модели оптимизации с использованием методов линейного программирования возможно применение приложения MS Excel, как в работах [2, 3]. Несмотря на ограничение использования данного метода линейными зависимостями, одним из его достоинств является возможность решения задач с множеством переменных и ограничений.

2.3 Нелинейное программирование

Работы [4–10] описывают применение методов нелинейного программирования на стадиях формирования требований и проектирования. Метод имитационного моделирования в работе [10] используется на стадии формирования требований. Как один из методов решения задач нелинейного программирования имеет значительное преимущество в виде множества автоматизированных реализаций. Также метод обладает наглядностью

и универсальностью. Однако для решения поставленной задачи использование метода предполагается несколько избыточным.

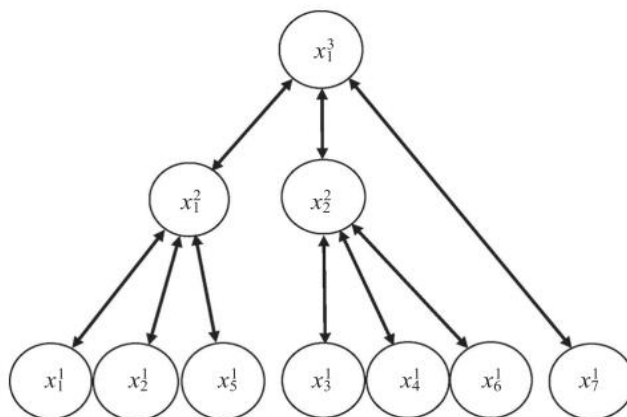


Рисунок 1. – Скорректированный (по результатам имитационного моделирования) вариант структуры системы управления [10]

2.4 Парето-оптимальная оценка и решения

Нахождение оптимальных решений по методу Парето – это графический вариант представления возможных вариантов выбора и ограничительных критериев, что делает его удобным инструментом для решения многокритериальных задач. Метод часто используют совместно с моделью «ящик Парето», моделью, отражающей диаграммы полезности двух показателей, позволяющей определять условия получения оптимального решения задачи, при достижении максимально возможного уровня полезности обоих показателей. В дальнейшем две модели объединены в принцип Эджворта – Парето. Множественные варианты применения и порядок использования принципа отражен в работах [11–16].

Преимуществом может послужить наглядность выбора и возможность для лица, принимающего решение оценить каждую из представленных альтернатив. Метод в работе [17] используется на стадии сопровождения. Одним из недостатков метода определяют ограниченность рассматриваемых показателей и вероятность нахождения оптимальных решений за пределами множества Парето.

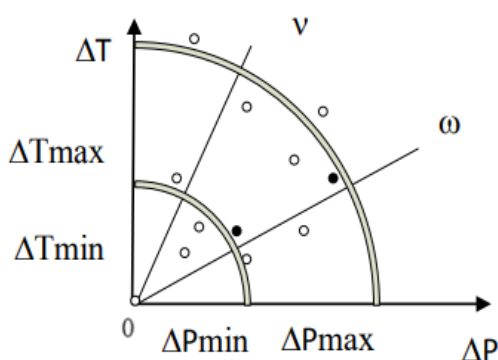


Рисунок 2. – Определение уровня фронта Парето при многокритериальной оптимизации решения [17]

2.5 Весовые коэффициенты

Матричный метод в работе [18] используется для представления возможных вероятностей исходов событий по отношению к количеству экспертов. При этом определение элементов матриц происходит с помощью многомерных производящих функций. Итоговая матрица отображает надежность проводимой экспертизы, что может быть использовано на любом из этапов создания СЗИ.

Для каждого из экспертов вероятности правильной классификации объектов могут быть описаны соответствующими квадратными вероятностными матрицами P_1, P_2, \dots, P_m , имеющими следующий вид:

$$P_j = \begin{pmatrix} p_{j11} & \dots & p_{j1k} \\ \dots & \dots & p_{j2k} \\ p_{jl1} & p_{jl2} & p_{jlk} \end{pmatrix}, j = 1, 2, \dots, m. \quad (5)$$

Метод анализа иерархий, в свою очередь, подразумевает расчет весовых коэффициентов для определений отношения предпочтения между показателями представленных альтернатив путем поиска собственного вектора. В работе [19] метод используется в процессе аудита, что позволяет применять его на этапах аттестации и сопровождения.

$$A = \begin{bmatrix} 1 & a_{12} & a_{13} \\ \frac{1}{a_{12}} & 1 & a_{23} \\ \frac{1}{a_{13}} & \frac{1}{a_{23}} & 1 \end{bmatrix} \quad (6)$$

Метод частично решает проблемы ранжирования факторов, присвоения коэффициентов факторам и прямой расстановки путем попарного сравнения значений матрицы коэффициентов. МАИ имеет свои недостатки, как, например, проблема согласованности коэффициентов [20].

Заключение

Так как методика предполагает использование математического аппарата в процессе принятия решений необходимо привести критерии к единой размерности. Далее рассчитываются коэффициенты с помощью МАИ. Путем расставления весовых коэффициентов критериям назначаются уровни предпочтения относительно друг друга, что в спорной ситуации поможет человеку, принимающему решение, склонится к тому или иному варианту (альтернативе).

Так как критериев несколько задача будет носить характер многокритериальной. МАИ позволяет свести множество неравенств, описывающих отношения альтернатив, критериев и ограничений к линейному уравнению. Решение линейного уравнения (R) по итогу отображается в виде гистограммы, которая будет иметь следующий вид, показанный на рисунке 3.

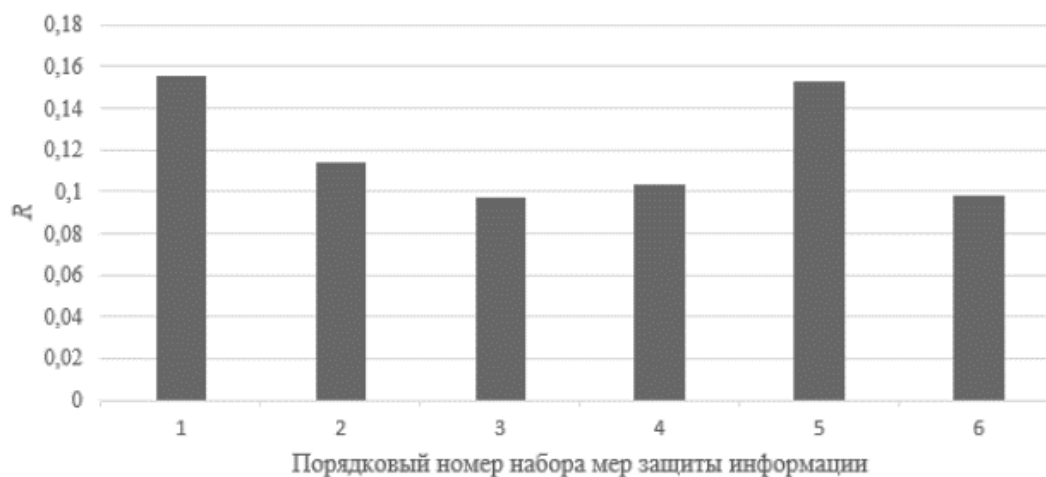


Рисунок 3. – Результаты вычисления функции

На рисунке 3 представлен график, полученный по результатам применения методики на экспериментальном макете.

Далее, по принципу Эджворта – Парето, выставляются ограничительные критерии и решение остается за лицом, принимающим решение. Либо выбирается значение в соответствии со значением параметра *extr*, минимальное или максимальное. Так как по определению указанного принципа, все точки, попавшие в область допустимых решений, являются оптимальными относительно друг друга.

Литература

1. Кулаков В.Г., Кобящев В.Г. Оптимальный синтез и анализ эффективности комплексов средств защиты информации. – Монография: г. Воронеж, ВГТУ, 2006. – 137 с.
2. Голенищев Э.П., Клименко И.В. К вопросу выбора инструментального средства для разработки программного обеспечения // Научно-образовательный журнал для студентов и преподавателей «StudNet». – 2022. – № 2. – С. 1083–1095.
3. Мейкшан В.И., Тесля Н.Б. Выбор оптимального размещения данных при использовании облачной инфраструктуры // Доклады Академии наук высшей школы Российской Федерации. – 2021, по. 2 (51). – pp. 34–42.
4. Кочегурова Е.А., Репина Е.Ю., Цехан О.Б. Гибридный подход для краткосрочного прогнозирования временных рядов на основе штрафного P-сплайна и эволюционной оптимизации // Компьютерная оптика. – 2020. – Т. 44, № 5. – С. 821–829.
5. Агафонов В.В., Зайцева Е.В., Яхеев В.В. Имитационное моделирование функциональных структур технологических систем угледобывающих предприятий // Уголь. 2022. – № 2. – С. 57–60.
6. Олейник, А.С. Методы и модели исследования и организации принятия решений по обеспечению комплексной безопасности важных государственных объектов // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2022. – № 42. – С. 194–212.
7. Тутов А.В., Тутова Н.В., Ворожцов А.С., Андреев И.А. Многокритериальная оптимизация размещения виртуальных машин по физическим серверам в облачных центрах обработки данных // Т-Comm: Телекоммуникации и транспорт, 2021. – Том 15, № 1. – С. 28–34.
8. Грибунин В.Г., Тимонов А.А. Об аналогии задач оптимизации выбора средств защиты информации с некоторыми задачами теории связи // Вопросы кибербезопасности. 2021. – № 5(45). – С. 30–35.
9. Кузьмин В.Н., Менисов А.Б. Исследование путей и способов повышения результативности выявления компьютерных атак на объекты критической информационной инфраструктуры. Информационно-управляющие системы, 2022. – № 4. – с. 29–43.
10. Онуфрей А.Ю., Разумов А.В., Какаев В.В. Метод оптимизации структуры в иерархических распределенных системах управления // Научно-технический вестник информационных технологий, механики и оптики, 2023. – Т. 23, № 1. – С. 44–53. doi: 10.17586/2226-1494-2023-23-1-44-53.
11. В. Д. Ногин, Обобщенный принцип Эджворта – Парето // Журнал вычислительной математики и математической физики. – 2015. – Том 55, № 12. – С. 2015–2021.
12. Ногин В.Д. Принцип Эджворта – Парето в терминах нечеткой функции выбора // Журнал вычислительной математики и математической физики. – 2006. – Т. 46. – № 4. – С. 582–591.
13. Noghin V.D. An Axiomatization of the generalized Edgeworth – Pareto principle in terms of choice functions // Math. Social Sciences. – 2006. – V. 52. – № 2. – P. 210–216.
14. Ногин В.Д, Волкова Н.А. Эволюция принципа Эджворта – Парето // Таврический вестник информатики и математики. – 2006. – № 1. – С. 23–33.
15. Подиновский В.В., Ногин В.Д. Парето-оптимальные решения многокритериальных задач. – М.: Наука. Главная редакция физико-математической литературы, 2007.

16. Ногин В.Д. Многокритериальный выбор на основе предпочтений ЛПР в многокритериальном режиме // Системный анализ в проектировании и управлении. – 2023. – С. 32–39.

17. Доронина Ю.В., Скатков А.В. Многокритериальный анализ статистической устойчивости системных характеристик информационно-телекоммуникационных каналов // Вестник Томского государственного университета. Управление, вычислительная техника и информатика, 2022. – № 60. – С. 59–72.

18. Бурков Е.А., Падерно П.И., Сатторов Ф.Э., Толкачева Е.А. Методологическая поддержка рабочей группы при решении задачи прогнозирования результатов классификационной экспертизы // Научно-технический вестник информационных технологий, механики и оптики.

19. Воеводин В.А., Маркин П.В., Маркина М.С., Буренок Д.С. Методика разработки программы аудита информационной безопасности с учетом весовых коэффициентов значимости свидетельств аудита на основе метода анализа иерархий // Системы управления, связи и безопасности. – 2021. – № 2. – С. 96–129.

20. Коробов В.Б., Тутыгин А.Г. Преимущества и недостатки метода анализа иерархий // Известия Российского государственного педагогического университета им. А.И. Герцена. – 2010 г. – С. 108–115.

НАУЧНО-ТЕХНИЧЕСКАЯ ПРОБЛЕМА КАТЕГОРИРОВАНИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

О.А. КОПЫРУЛИНА

*Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»,
г. Санкт-Петербург*

Введение

С каждым годом значимость и распространение информационных технологий растет. Применение компьютерной техники позволяет оптимизировать различные бизнес-процессы, тем самым увеличивая производительность или сокращая издержки. Хотя ИТ (информационные технологии) являются полезным инструментом в ведении деятельности любой организации, физические объекты, такие как автоматизированные рабочие места (АРМ), ноутбуки, маршрутизаторы и т.п., также становятся объектами воздействия хакерских атак. Действительно, выход из строя определенных автоматизированных рабочих мест, например, тех, которые обслуживают критические процессы, может привести к полной остановке деятельности предприятия, что естественно приведет к финансовым потерям.

Стоит учитывать, что при проведении целевых преднамеренных атак, возможен ущерб не только для организаций, на которые была реализована атака, но и даже всему государству. Это могут быть проблемы с рабочими местами после закрытия предприятия, экологические катастрофы, срывы оборонных заказов и многие другие последствия. Осознавая возможность подобного развития ситуации, в Российской Федерации была проведена работа по законодательному регулированию.

В 2018 году вступил в силу Федеральный Закон № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017, который регулирует меры по обеспечению информационной безопасности на критически важных объектах. С выходом данного закона на повестку дня специалистов по информационной безопасности предприятий встал вопрос об обеспечении безопасности ЗОКИИ [3]. Для того чтобы выявить ЗОКИИ (значимые объекты критической информационной инфраструктуры), а также обеспечить оптимальные меры по их защите, необходимо провести категорирование [2]. В настоящий момент категорирование ОККИ (объектов критической информационной инфраструктуры) происходит согласно 127 ПП (постановления Правительства), в котором угрозы безопасности для ОККИ, а, следовательно, и риски учитываются не в полной мере, что влечет за собой невозможность объективного присвоения категории. Поэтому важно признавать актуальность данной проблемы и обеспечить детальный и непрерывный анализ и оценку рисков еще на этапе категорирования. Также зачастую специалист, занимающийся данным процессом, тратит слишком много временных ресурсов на составление документации по категорированию. Этим обуславливается актуальность данной работы.

1. Степень разработанности темы исследования

В условиях компьютеризации всех областей человеческой деятельности имеется острая необходимость в защите от угроз информационной безопасности. Особенно актуально это для объектов, вывод из строя которых может привести к огромному ущербу для общества, государства, обороны, политики или же экономики. Таковыми являются объекты критической информационной инфраструктуры. Для того чтобы выявить значимые объекты критической информационной инфраструктуры, а также обеспечить оптимальные меры по защите, необходимо провести категорирование. Зачастую специалист, занимающийся данным процессом, тратит слишком много временных ресурсов на составление документации по категорированию.

На рисунке 1 более подробно представлены сферы деятельности субъектов КИИ.

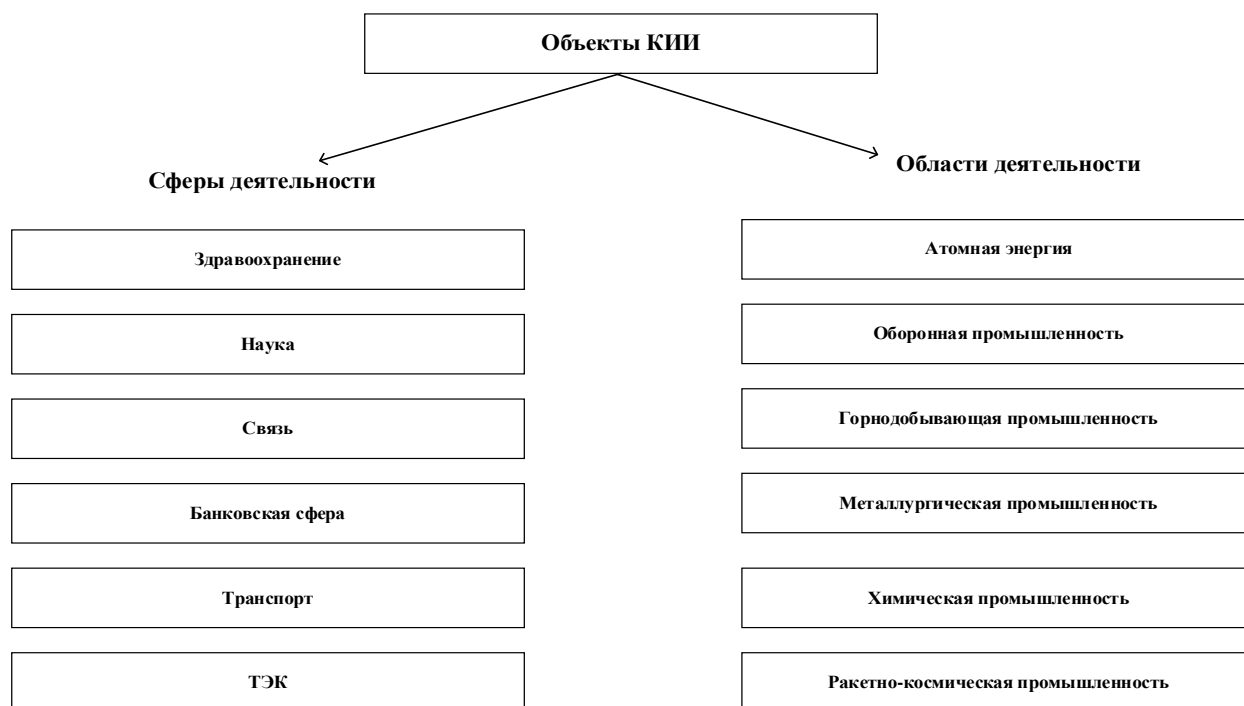


Рисунок 1. – Сферы функционирования объектов КИИ

Если предприятие попадает под одну из сфер КИИ, то оно является субъектом КИИ, а, следовательно, содержит объекты, требующие особого внимания и категорирования. На основании данного закона составляется перечень объектов, подлежащих категорированию, и отправляется во ФСТЭК. Далее они вносятся в реестр [2].

По мнению академика В. А. Легасова, свыше 60 % аварий происходит из-за ошибок персонала «рисковых» объектов [1]. Таким образом, выявление критически значимых объектов, а также присвоение им правильной категории является важной составляющей защиты этих объектов. В таблице 1 представлен перечень работ, выполняемых при проведении категорирования объектов КИИ.

Таблица 1. – Перечень работ при категорировании объектов КИИ

№ п/п	Наименование этапа работ	Наименование выполняемых работ
1	Сбор сведений об объектах КИИ	Сбор сведений о субъекте КИИ
		Определение процессов, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта КИИ
		Выявление наличия критических процессов у субъекта КИИ
		Выявление объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов

№ п/п	Наименование этапа работ	Наименование выполняемых работ
2	Анализ возможных действий нарушителей в отношении объектов КИИ	Рассмотрение возможных действий нарушителей в отношении объектов КИИ, а также иных источников УБИ
		Определение внешних и внутренних нарушителей; определение возможных действий нарушителей; расчет актуальности нарушителей
		Анализ УБИ, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ
		Формирование перечня актуальных УБИ для рабочих материалов по категорированию объекта КИИ
		Оценка в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ, определение значения каждого из показателей критериев значимости или обоснование их неприменимости
		Установление каждому из объектов КИИ одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им категорий значимости
		Оформление актов категорирования объектов КИИ
3	Подготовка отчетных документов	

2. Разработка метода процесса категорирования объектов КИИ

Метод процесса категорирования объектов КИИ представлен на рисунке 2.

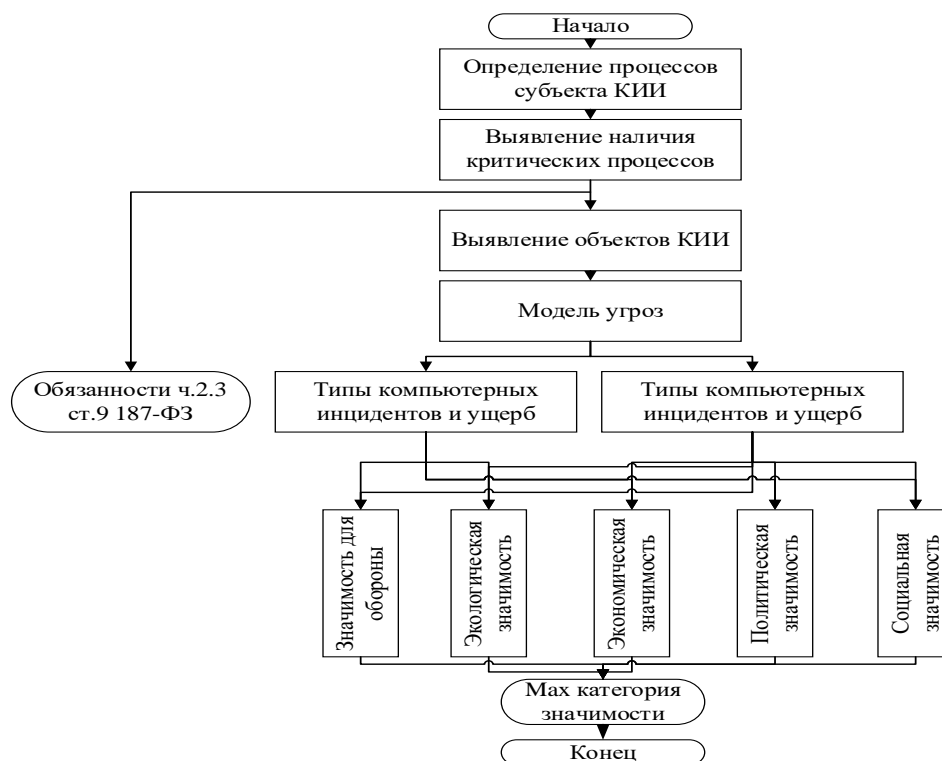


Рисунок 2. – метод процесса категорирования объектов КИИ

Существующие подходы по категорированию не учитывают всех возможных рисков возникновения УБИ на ОКИИ. Например, ЗОКИИ может быть присвоена 1 категория значимости, однако, риск возникновения УБИ настолько мал, что все меры защиты для 1 категории просто не нужны. Или наоборот, для ЗОКИИ 3 категории необходимы более совершенные меры защиты, так как риски возникновения УБИ очень велики. Также существующие подходы требуют очень больших временных затрат на разработку актов категорирования, однако в данном случае каждая минута специалиста ценна и затягивание в проведении категорирования ОКИИ может привести к непоправимым последствиям. Например, незащищенный объект может быть взломан хакерскими группировками и с помощью него нанесен ущерб в одной или нескольких областях человеческой деятельности.

Сложность категорирования, а также необходимость точности присвоения категории ЗОКИИ диктует необходимость разработки эффективной модели категорирования ОКИИ. Очевидно, что предлагаемая модель должна учитывать основные факторы, влияющие на присвоение категории ЗОКИИ: социальную значимость, экономическую значимость, политическую значимость, значимость для обороны страны и безопасности государства, экологическую значимость, а также риски возникновения УБИ.

Для уменьшения временных затрат, специалиста, занимающегося категорированием, необходимо как можно больше автоматизировать данный процесс. Таким образом необходимо разработать программный продукт, который будет выдавать готовые результаты. Подобный подход является наиболее перспективным.

Заключение

Существующие подходы по категорированию не учитывают всех возможных рисков возникновения УБИ на ОКИИ. Например, ЗОКИИ может быть присвоена 1 категория значимости, однако, риск возникновения УБИ настолько мал, что все меры защиты для 1 категории просто не нужны. Или, наоборот, для ЗОКИИ 3 категории необходимы более совершенные меры защиты, так как риски возникновения УБИ очень велики. Также существующие подходы требуют очень больших временных затрат на разработку актов категорирования, однако в данном случае каждая минута специалиста ценна и затягивание в проведении категорирования ОКИИ может привести к непоправимым последствиям. Например, незащищенный объект может быть взломан хакерскими группировками и с помощью него нанесен ущерб в одной или нескольких областях человеческой деятельности.

Сложность категорирования, а также необходимость точности присвоения категории ЗОКИИ диктует необходимость разработки эффективной модели категорирования ОКИИ. Очевидно, что предлагаемая модель должна учитывать основные факторы, влияющие на присвоение категории ЗОКИИ: социальную значимость, экономическую значимость, политическую значимость, значимость для обороны страны и безопасности государства, экологическую значимость, а также риски возникновения УБИ.

Для уменьшения временных затрат, специалиста, занимающегося категорированием, необходимо автоматизировать данный процесс. Таким образом, необходимо разработать программный продукт, который будет выдавать готовые результаты. Подобный подход является наиболее перспективным.

Литература

1. Акимов В.А. и др. Надежность технических систем и техногенный риск: Учебное пособие. Под общей редакцией М.И. Фалеева. – М.: «Деловой Экспресс». 2002. – 368 с.
2. Постановление Правительства РФ «Об утверждении правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений» от 8 февраля 2018 № 127 // Российская газета. – 2018 г.
3. Федеральный Закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 № 187-ФЗ // Российская газета. – 2017 г.

ПОРЯДОК КАТЕГОРИРОВАНИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ НА ПРИМЕРЕ ТЭК

О.А. КОПЫРУЛИНА

*Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»,
г. Санкт-Петербург*

Введение

Проблема реализации требований 187-ФЗ на данный момент актуальна и широко обсуждается, так как отсутствует практический опыт реализации нормативных требований, а также изданные нормативно-правовые акты проработаны не до конца.

1. Оценка уязвимостей объектов критической информационной инфраструктуры

В настоящий момент известны следующие системы оценки уязвимостей:

- CWE (Common Weakness Enumeration) [3];
- CVSS (Common Vulnerability Scoring System) [1];
- NIAC (National Infrastructure Advisory Council) [5];
- OWASP (Open Web Application Security Project) [6];
- Microsoft Rating System [2];
- Korea Internet & Security Agency [4].

Open Web Application Security Project

Система оценки уязвимостей OWASP представляет собой базу, содержащую более 500 тыс. уязвимостей. Несмотря на то что данный проект не является официальным стандартом, а носит лишь информационный характер, он широко используется организациями в сфере кибербезопасности для классификации уровня опасности уязвимостей.

Microsoft Rating System

Структурированный список уязвимостей по 4 классам представляет из себя система Microsoft Rating System. Оценки уязвимостей представляются по различным продуктам компании Microsoft.

Common Vulnerability Scoring System

CVSS представляет из себя открытую схему, позволяющую обмениваться уязвимостями. Основная цель данной системы – предоставить возможность специалистам в сфере безопасности обмениваться информацией о найденных уязвимостях.

Проблемы моделирования УБИ для ОКИИ

В работе Лим В.Г. «Моделирование угроз информационной безопасности в АСУ предприятия топливно-энергетического комплекса» рассматриваются вопросы обеспечения ИБ в ТЭК. Предложена методика построения модели угроз в АСУ ТП для объектов ТЭК [8].

В работе Корнеева А.В. «Защита инфраструктуры ТЭК от новых средств кибернетического нападения. Опыт борьбы с дистанционным терроризмом» рассматриваются внутренние производственные, технические и финансовые риски для предприятий ТЭК. Ввиду развития современных технологий эта тема достаточно актуальна [7].

Необходимо отметить, что зачатую ПО на АСУ ТП не обновляется годами из-за необходимости непрерывной работы, что влечет за собой развитие новых угроз.

В существующей нормативной базе нет ясных требований к таким ОКИИ как АСУ ТП. Требования по защите от НСД, согласно ФСТЭК России, не учитывали множество вопросов, таких как сигнализация попыток нарушения защиты, контроль доступа субъектов и программ, узлам сети, каналам связи и др.

Порядок категорирования ОКИИ на примере ТЭК

Как говорилось ранее, в отношении определения актуальности УБИ существует весьма обширная практика ФСТЭК и ФСБ. Однако, чтобы оценить защищенность активов на данный момент и более точно присвоить категорию ОКИИ необходимо применить риск-ориентированные стандарты такие как: ISO серии 27001, 55001, 20000, 22301, ГОСТ Р 54336-2011 Системы экологического менеджмента в организациях, выпускающих нанопродукцию, ГОСТ Р 54338-2011 Системы менеджмента качества в организациях, выпускающих нанопродукцию. Также стоит отметить практику применения отраслевых стандартов: СТО БР ИББС (Банка России), СТО ПАО «Газпром».

Возьмем в пример объекты КИИ топливно-энергетического комплекса. Согласно стандарту ISO 27001 выделяются следующие требования:

- «высшее руководство должно демонстрировать лидерство»;
- «организация должна выполнять планы по достижению целей ИБ, как определено в п. 6.2.»;
- «система менеджмента ИБ организации должна включать документированную информацию»;
- «организация должна предоставить необходимые ресурсы».

В ФЗ-187 [9] в ст. 7 определены требования к категорированию объектов КИИ: «Субъекты критической информационной инфраструктуры в соответствии с критериями значимости и показателями их значений, а также порядком осуществления категорирования присваивают одну из категорий значимости принадлежащим им на праве собственности, аренды или ином законном основании объектам критической информационной инфраструктуры. Если объект критической информационной инфраструктуры не соответствует критериям значимости, показателям этих критериев и их значениям, ему не присваивается ни одна из таких категорий». Для выполнения этой нормы ФЗ-187 [9] применимы следующие требования ISO 27001:

- «активам, приведенным в реестре активов, должны быть определены владельцы»;
- «правила допустимого использования информации и активов, связанных с информацией и средствами для обработки информации, должны быть определены, документированы и внедрены»;
- «изменения в организации, средствах и системах обработки информации, влияющих на ИБ, должны контролироваться»;
- «использование ресурсов должно быть контролируемым».

Основными современными риск-ориентированными подходами являются: ISO 31000, NIST, OCTAVE, FAIR, IATA.

Для каждой отрасли подойдет свой риск-ориентированный подход. После построения модели угроз и оценки рисков для ОКИИ можно проводить непосредственно категорирование.

Заключение

Для каждой отрасли подойдет свой риск-ориентированный подход. После построения модели угроз и оценки рисков для ОКИИ можно проводить непосредственно категорирование.

Список литературы

1. Common Vulnerability Scoring System // Википедия URL: https://ru.wikipedia.org/wiki/Common_Vulnerability_Scoring_System (дата обращения: 11.03.2023).
2. Comparing and Evaluating CVSS Base Metrics and Microsoft Rating System // researchgate URL: https://www.researchgate.net/publication/278784873_Comparing_and_Evaluating_CVSS_Base_Metrics_and_Microsoft_Rating_System (дата обращения: 11.03.2023).
3. CWE // Common Weakness Enumeration URL: <https://cwe.mitre.org/> (дата обращения: 11.03.2023).
4. Korea Internet & Security Agency // kisa URL: <https://www.kisa.or.kr/EN> (дата обращения: 11.03.2023).

5. National Infrastructure Advisory Council // Википедия URL: https://en.wikipedia.org/wiki/National_Infrastructure_Advisory_Council (дата обращения: 11.03.2023).
6. Who is the OWASP Foundation // OWASP URL: <https://owasp.org/> (дата обращения: 11.03.2023).
7. Корнеев, А.В. Защита инфраструктуры ТЭК от новых средств кибернетического нападения: опыт борьбы с дистанционным терроризмом // Энергобезопасность и энергосбережение. – 2012. – № 1. – С. 5–10.
8. Лим В.Г., Арбузов Ю.А., Химич В.Н., Дзиев С.К. Моделирование угроз информационной безопасности в АСУ предприятия топливно-энергетического комплекса // Вопросы защиты информации. – 2010. – № 3. – С. 23–27.
9. Федеральный Закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 № 187-ФЗ // Российская газета. – 2017 г.

ПРОБЛЕМЫ ПРИ ФОРМИРОВАНИИ МОДЕЛЕЙ ПРОЦЕССА КАТЕГОРИРОВАНИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

О.А. КОПЫРУЛИНА

*Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»,
г. Санкт-Петербург*

Введение

Прежде всего, возникает необходимость в рассмотрении существующего законодательства для определения законодательных требований. Законодательство включает в себя: Федеральные законы и постановления Правительства.

Проблема реализации требований 187-ФЗ на данный момент актуальна и широко обсуждается, так как отсутствует практически опыт реализации нормативных требований, а также изданные нормативно-правовые акты проработаны не до конца.

В статье Шабурова А.С., Двойнишникова Н.Э., Шлыкова А.И «Особенности реализации требований по категорированию объектов критической информационной инфраструктуры» рассматривается проблема неоднозначности определения категории ОКИИ. Согласно данной статье показатель 2 и 3 категории ОКИИ не может быть определен корректно, исходя из границ их значений. Авторы предлагают изменить последовательность этапов категорирования ОКИИ и первым этапом сделать составление перечня ОКИИ, подлежащих категорированию. Смена этапов обуславливается тем, что в комиссию по категорированию нужно включать только осведомленных специалистов [5]. Данная позиция достаточно интересна, однако возникает вопрос: если комиссия не назначена, кто будет уполномочен в правильном составлении перечня ОКИИ?

В статье Котова А.А, Куринной В.С, Шлыкова М.С «Алгоритм категорирования объектов критической информационной инфраструктуры» рассматривается проблема алгоритмизации процесса категорирования ОКИИ. Авторы предлагают алгоритм, согласно которому значительно снижаются затраты на категорирование ОКИИ. Также в статье говорится о четырех категориях значимости, хотя всем известно, что законодательно закреплены три категории. Под четвертой категорией подразумевается отсутствие необходимости присвоения категории [2].

Дегтерев Р.Э. в своей статье «Разработка автоматизированной системы категорирования объектов критической информационной инфраструктуры на примере Евраз НТМК» рассматривает необходимость автоматизации процессов категорирования ОКИИ металлургических предприятий. Автор предлагает автоматизировать часть процесса категорирования ОКИИ [1]. Однако, данный вариант автоматизации сокращает лишь часть временных затрат специалиста, большинство этапов необходимо делать вручную.

Анализ данных работ дает полную картину противоречий между различными авторами, нормативно-методической базой ФСТЭК России и практики реализации этого процесса в жизни.

1. Проблемы при формировании моделей процесса категорирования объектов критической информационной инфраструктуры

На практике субъекты КИИ сталкиваются со следующими проблемами:

- избыточность и сложность процедур, требуемых для выполнения постановления Правительства № 127;
- действия нарушителей в отношении объектов КИИ, УБИ и уязвимостей никак не влияют на итоговую категорию;
- нестабильность требований постановления Правительства № 127 и приказов ФСТЭК России.

В настоящее время большинство организаций в процессе категорирования руководствуется либо публичными разъяснениями ФСТЭК России, либо локальными методическими документами, разработанными самостоятельно под определенную отрасль.

Однако существует значительное противоречие. ФСТЭК России рекомендует определять объект КИИ исходя из сферы деятельности субъекта, но идентифицировать однозначно объекты КИИ предложенными методами практически невозможно.

Возникает ряд вопросов:

– предположим, что организация осуществляет свою деятельность в одной из указанных сфер, но ее процессы не автоматизированы, то есть информационных систем нет, что будет являться объектами КИИ?

– многие организации, попадающие под перечень сфер, пользуются услугами подрядчиков и не имеют собственных ИС, как быть в этом случае?

– также стоит учитывать во внимание организации, не осуществляющие свою деятельность в указанных сферах, но имеющие ИС, функционирующие в указанных сферах деятельности, являются ли они ЗОКИИ?

В форму уведомления и в реестр значимых объектов КИИ вносится информация исключительно по сферам деятельности объекта КИИ, а не субъекта.

1.1. Избыточность и сложность процедур, требуемых для выполнения постановления Правительства № 127

На основании Федерального закона № 187 [4] можно сделать выводы, что категорирование ОКИИ это не что иное, как соответствие ОКИИ критериям значимости и показателям, присвоение объекту одной из категорий значимости, а также проверку результатов присвоения. В постановлении правительства № 127 [3] введены дополнительные обязанности для субъекта КИИ, усложняющие определение категорий значимости, но не оказывающие влияние на итоговую категорию.

Таким образом, появляется следующее противоречие: субъект КИИ обязан вначале выявить ОКИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, но ФЗ-187 указывает, что обязательно категорирование всех без исключения ОКИИ.

Также в постановлении правительства № 127 [3] существует формулировка о необходимости согласования перечня объектов КИИ с государственным органом или российским юридическим лицом, которая зачастую воспринимается субъектом КИИ как необходимость согласования с ФСТЭК России. При этом в 187-ФЗ [4] и подзаконных актах в данных организациях работа по рассмотрению и оценке полученных от подведомственных субъектов КИИ перечней объектов КИИ не предусмотрена. Это приводит к низкой эффективности процедуры согласования перечней объектов КИИ и большим временным потерям на служебную переписку между организациями и подведомственными им субъектами КИИ.

Также документы по результатам категорирования (акт и форма уведомления о результатах категорирования) дублируют друг друга.

1.2. Действия нарушителей в отношении объектов КИИ, УБИ и уязвимостей никак не влияют на итоговую категорию

Согласно ПП 127 субъект КИИ обязан провести анализ возможных действий нарушителей в отношении ОКИИ, УБИ и уязвимостей, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ. При этом результаты проведенного анализа никак не используются при установлении каждому из ОКИИ одной из категорий значимости либо принятии решения об отсутствии необходимости присвоения категорий значимости.

Таким образом, ЗОКИИ может быть недостаточно защищен от действий злоумышленников или же наоборот, некоторые меры защиты могут быть излишне, что повлечет за собой необоснованные расходы.

1.3. Нестабильность требований постановления Правительства № 127 и приказов ФСТЭК России

Изначально редакция постановления Правительства № 127 [3] содержала ошибки в нескольких показателях критериев значимости.

На текущий момент ФСТЭК России решила не просто исправить ошибки в постановлении правительства № 127 [3], а внести радикальные изменения в процессы категорирования: изменены принципы создания и расформирования комиссии по категорированию субъекта КИИ, радикально занижены пороговые показатели категорий значимости для сфер транспорта и связи. В плановом порядке вносятся также изменения в приказ ФСТЭК России об оформлении результатов категорирования.

Таким образом, вышеперечисленные проблемы значительно увеличивают временные затраты специалиста, занимающегося категорированием ЗОКИИ.

Заключение

Для усовершенствования процесса категорирования ЗОКИИ необходимо:

1. Исключить избыточные этапы, не оказывающие влияния на определение показателей категорий значимости объектов КИИ:

– составление перечня объектов, подлежащих категорированию, и последующих действий с ним.

2. Этап оформления акта категорирования объекта КИИ заменить на заполнение формы уведомления о результатах категорирования.

3. Создать единый метод категорирования ЗОКИИ и ПО для автоматизации процесса категорирования, учитывая влияние действий нарушителей в отношении объектов КИИ, УБИ и уязвимостей на итоговую категорию значимости.

Литература

1. Дегтерев, Р.Э. Разработка автоматизированной системы категорирования объектов критической информационной инфраструктуры на примере ЕВРАЗ НТМК / Р.Э. Дегтерев // Теплотехника и информатика в образовании, науке и производстве: сборник докладов VIII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых (ТИМ'2019) с международным участием, Екатеринбург, 16–17 мая 2019 года / Министерство науки и высшего образования и Российской Федерации, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, Институт новых материалов и технологий, Кафедра «Теплофизика и информатика в металлургии». – Екатеринбург: ООО АМК «День РА», 2019. – С. 239–244.

2. Котов, А.А. Алгоритм категорирования объектов критической информационной инфраструктуры / А.А. Котов, В.С. Куринная, М.С. Шлыков // REDS: Телекоммуникационные устройства и системы. – 2018. – Т. 8. – № 4. – С. 34–37.

3. Постановление Правительства РФ «Об утверждении правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений» от 8 февраля 2018 № 127 // Российская газета. – 2018 г.

4. Федеральный Закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 № 187-ФЗ // Российская газета. – 2017 г.

5. Шабуров, А.С. Особенности реализации требований по категорированию объектов критической информационной инфраструктуры / А.С. Шабуров, Н.Э. Двойнишников, А.И. Шлыков // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 4(30). – С. 75–82. – DOI 10.14529/secur180411.

АЛГОРИТМЫ РАЗРАБОТКИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОБЛАЧНЫХ РЕСУРСОВ

В.П. КОЧИН, А.В. ШАНЦОВ

*Белорусский государственный университет,
г. Минск, Республика Беларусь*

Введение

Эффективная защита информационных ресурсов (далее – ИР), использующих облачные ресурсы (далее – ОР), достигается путем создания комплексной системы защиты информации (далее – СЗИ) [1]. Требования к построению комплексной СЗИ определяются требованиями законодательных актов [2], а также уточняются по результатам выполнения процедур инвентаризации активов ИР и оценки рисков. Однако, большинство из методик разработки СЗИ не учитывают влияние облачных вычислений на процесс обеспечения информационной безопасности [3]. Для создания и поддержания в актуальном состоянии СЗИ облачные провайдеры и облачные потребители должны применять алгоритмы построения СЗИ, учитывающие особенности функционирования ОР. В настоящей работе рассматриваются два алгоритма по созданию СЗИ для облачных провайдеров и облачных потребителей.

Алгоритм разработки системы защиты информации для облачных провайдеров

Облачный провайдер несет ответственность за защищенность ОР в целом. СЗИ облачной платформы должна разрабатываться с учетом требований безопасности к максимально допустимой категории обрабатываемых активов и обеспечивать защищенность активов согласно требованиям законодательных актов. Алгоритм разработки СЗИ для ОР для облачных провайдеров состоит из шести шагов и представлен на рисунке 1.



Рисунок 1. – Алгоритм разработки СЗИ для облачных провайдеров

Ниже приводится подробное описание шагов данного алгоритма.

Шаг 1: категорирование ОР. При категорировании ОР определяется максимально допустимая категория обрабатываемых активов (ИР) в ОР.

Шаг 2: выбор базового набора средств защиты информации. Выбор базового набора осуществляется исходя из требований законодательства [2] и должен соответствовать требованиям для наивысшей категории активов, обрабатываемых в ОР.

Шаг 3: разработка моделей нарушителя и угроз, оценка рисков для ОР. Разрабатываемые модели должны учитывать особенности обработки активов на облачных платформах [4]. Оценка рисков должна быть направлена на идентификацию всех возможных угроз и оценки вероятности их реализации [5].

Шаг 4: оценка достаточности базового набора средств защиты информации, внедрение дополнительных средств защиты (при необходимости). Исходя из разработанных моделей нарушителя и угроз, оценки рисков для ОР, облачный провайдер должен оценить достаточность базового набора средств защиты информации. В случае его недостаточности – внедрить дополнительные средства (меры) защиты информации.

Шаг 5: ввод в эксплуатацию СЗИ ОР. На этом этапе внедряются все выбранные средства защиты информации, проверяется их соответствие заявленным требованиям и работоспособность в целом в составе СЗИ. При необходимости проводится аудит СЗИ, включающий в том числе тестирование на проникновение.

Шаг 6: мониторинг состояния СЗИ. Мониторинг состояния СЗИ включает в себя непрерывную оценку соответствия СЗИ необходимому уровню защиты для ОР. Оценка соответствия должна осуществляться по следующим критериям: соответствие средств защиты информации и СЗИ в целом заданным требованиям, соответствие СЗИ требованиям законодательных актов, соответствие СЗИ моделям нарушителя и угроз.

При изменении категории обрабатываемых активов, изменении требований законодательных актов, облачный провайдер должен вернуться к шагу 1 или шагу 2 алгоритма соответственно и повторно выполнить все оставшиеся шаги. Также облачный провайдер должен периодически, но не реже одного раза в три года, уточнять модели нарушителей и угроз. После уточнения указанных моделей (шаг 4 алгоритма), облачный провайдер должен повторно выполнить все оставшиеся шаги алгоритма.

Алгоритм разработки системы защиты информации для потребителей облачных услуг

Потребитель облачных услуг несет полную ответственность за сохранность данных пользователей при их обработке и хранении в ИР. Следовательно, облачным потребителям, при переносе их ИР на облачную платформу, необходимо также создавать собственную СЗИ, гарантирующую сохранность данных пользователей при их обработке и хранении в ИР. Алгоритм разработки СЗИ для облачных потребителей имеет отличия от алгоритма для облачных провайдеров. Данный алгоритм включает в себя семь шагов и представлен на рисунке 2.

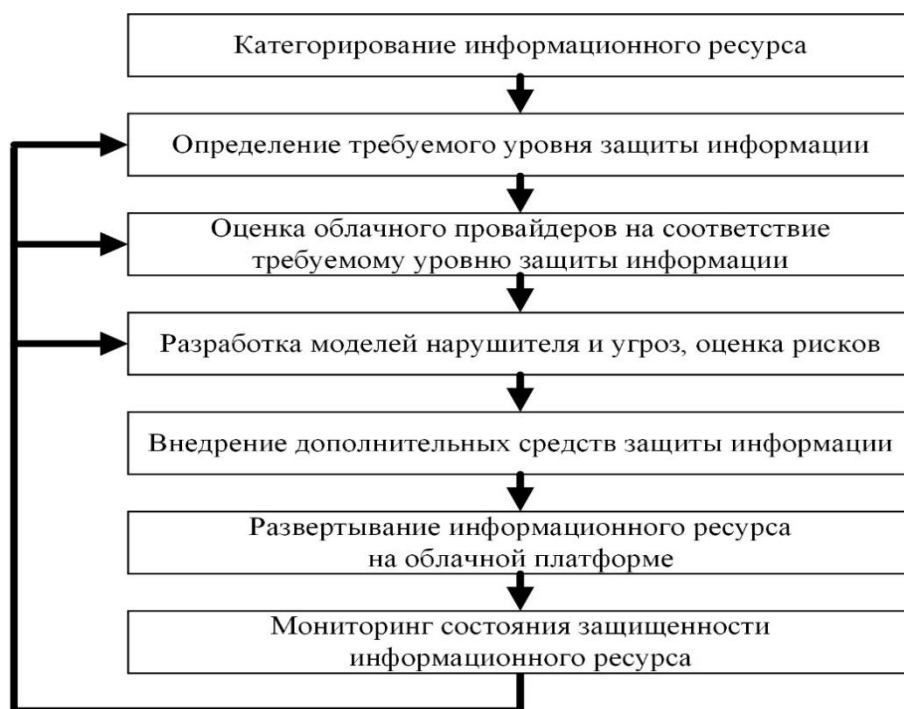


Рисунок 2. – Алгоритм разработки СЗИ для потребителей облачных услуг

Детальное рассмотрение алгоритма разработки СЗИ для потребителей облачных услуг представлено ниже.

Шаг 1: категорирование ИР. Категорирование ИР должно осуществляться в соответствии с законодательными актами [2].

Шаг 2: определить требуемый уровень защиты информации. Исходя из категории ИР, облачный потребитель должен определить требуемый уровень защиты информации.

Шаг 3: оценить облачного провайдера на соответствие требуемому уровню защиты информации. Оценка облачного провайдера должна осуществляться путем рассмотрения аттестатов ОР, уточнения договора об уровне обслуживания. В отдельных случаях оценка проводится путем независимого аудита ОР.

Шаг 4: разработка моделей нарушителя и угроз, оценка рисков. Указанные процедуры должны осуществляться независимо от разработанных моделей и оценки рисков облачного провайдера и должны учитывать специфику данного ИР.

Шаг 5: внедрение дополнительных средств защиты информации. Исходя из оценки СЗИ облачного провайдера, разработанных моделей нарушителя и угроз для ИР, оценки рисков потребитель облачных услуг при необходимости дополнительно внедряет собственные средства защиты информации. Дополнительные средства защиты информации внедряются с помощью облачного провайдера либо непосредственно облачным потребителем.

Шаг 6: развертывание (перенос) ИР на облачной платформе. После выполнения всех процедур по оценке защищенности ИР и внедрении дополнительных средств защиты информации облачный потребитель осуществляет развертывание ИР на облачной платформе.

Шаг 7: мониторинг состояния защищенности ИР. Мониторинг состояния защищенности ИР включает: непрерывный контроль за функционированием собственных средств защиты информации, отслеживание изменений в законодательных актах и изменений аттестатов ОР, периодическое уточнение моделей нарушителя и угроз для ИР.

При изменении законодательных актов облачному потребителю необходимо перейти к шагу 2 алгоритма, при изменении аттестатов ОР необходимо перейти к шагу 3, после уточнения моделей нарушителя и угроз – к шагу 4 алгоритма соответственно.

Заключение

СЗИ облачных платформ должна в обязательном порядке учитывать специфику облачных вычислений [6], вместе с тем, СЗИ должна в полном объеме соответствовать требованиям законодательных актов Республики Беларусь. Представленные алгоритмы разработки СЗИ ОР и ИР, функционирующих на облачных платформах, учитывают требования существующих законодательных актов Республики Беларусь и особенности функционирования облачных платформ. Данные алгоритмы используют подход, основанный на применении базового набора средств защиты информации, согласно требованиям законодательных актов, и дополнительных средств защиты информации, учитывающих специфику активов и особенности облачных вычислений. Указанные особенности алгоритмов разработки СЗИ позволяют создавать комплексные СЗИ, обеспечивающие максимально эффективный уровень защищенности активов при минимально возможных затратах на развертывание и внедрение средств защиты информации.

Литература

1. Кочин В.П. Комплексная система защиты информации облачных ресурсов. / В.П. Кочин, А.В. Шанцов // Комплексная защита информации: материалы XXVI научно-практической конференции, Минск, 25–27 мая 2021 г. / НП РУП «Научно-исследовательский институт технической защиты информации» – Минск, 2021. – С. 332–334.
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>
3. Кочин В.П. Проблемы проектирования комплексной системы защиты информации облачных ресурсов в Республике Беларусь / В.П. Кочин, А.В. Шанцов // Цифровая трансформация. 2021; № 3: 34–39.
4. Кочин В.П. Разработка модели нарушителя облачных ресурсов / В.П. Кочин, А.В. Шанцов // Управление информационными ресурсами: материалы XIX Международной научно-практической конференции, Минск, 22 марта 2023 г. / Академия управления при Президенте Республики Беларусь: Минск, 2023. – С. 244–246.
5. Информационные технологии. Методы и средства безопасности. Методика оценки рисков информационной безопасности в информационных системах: СТБ 34.101.70-2016. – Введ. 12.08.16. – Минск: Белорус. гос. ин-т стандартизации и сертификации, 2016.
6. Кочин В.П. Особенности построения комплексной системы защиты информации облачных ресурсов / В.П. Кочин, А.В. Шанцов // Научная конференция студентов и аспирантов Белорусского государственного университета: материалы 78-й научной конференции студентов и аспирантов БГУ, Минск, 2021. – С. 103–106.

ЗАЩИТА ДАННЫХ В ЭПОХУ КВАНТОВЫХ КОМПЬЮТЕРОВ: ВАЖНОСТЬ ПЕРЕХОДА НА ПОСТКВАНТОВУЮ КРИПТОГРАФИЮ

М.А. НАУМОВ

*Научно-производственное республиканское унитарное предприятие
Научно-исследовательский институт технической защиты информации,
Минск, Республика Беларусь*

В настоящее время сложно представить передачу конфиденциальной информации между информационными системами без применения средств криптографической защиты информации. Совместное использование симметричных и асимметричных криптографических алгоритмов позволяет обеспечивать защиту передаваемых данных с заданным уровнем стойкости. Однако не все принимают во внимание возрастающую угрозу применения квантовых компьютеров для атак на уязвимые криптографические алгоритмы асимметричного шифрования, выработки и проверки электронной цифровой подписи.

В рамках исследовательских целей целесообразно рассмотреть сравнение скоростей работы современных криптографических алгоритмов. Были рассмотрены некоторые алгоритмы и построен соответствующий график зависимостей, показанный на рисунке 1 [2].

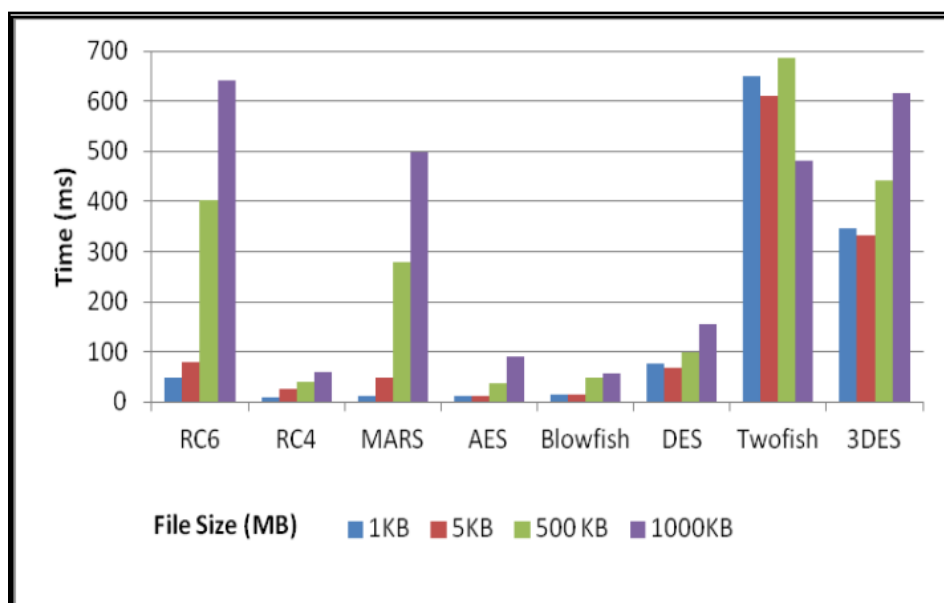


Рисунок 1. – Сравнение времени шифрования/расшифрования различных алгоритмов

После проведения анализа существующих криптографических методов (алгоритмов) справедливо сделать вывод, что по криптостойкости и скорости шифрования/расшифрования наилучшим выбором из рассматриваемых алгоритмов будет AES (Rijndael).

Отдельно был рассмотрен сравнительный анализ стандарта ГОСТ Р 34.12-2015 и стандарта шифрования AES, на основании которого были замечены недостатки ГОСТ Р 34.12-2015 по сравнению со стандартом AES как в скорости, так и в криптостойкости [3].

Современная криптография во многом полагается на асимметричные алгоритмы. Их основной принцип базируется на функциях, которые легко вычисляются, но трудно обращаются. По сути, они являются условно односторонними из-за большой асимметрии в сложности (RSA, DSA, ECDSA). Задачи обращения таких функций имеют суб-экспоненциальную или экспоненциальную сложность, например, задачи факторизации и дискретного логарифмирования. У этих алгоритмов есть один недостаток – они сравнительно медленные, и их аппаратное ускорение сложнее реализовать. Поэтому шифрование всего трафика между двумя узлами с использованием только асимметричной

криптографии возможно, но бессмысленно из-за низкой производительности и большой нагрузки. Классический подход подразумевает использование «дорогих» асимметричных алгоритмов только для проверки подлинности сертификата и выработки общего сеансового ключа, который используется при шифровании основного объема данных с помощью симметричной криптосистемы. Современные подходы к шифрованию подразумевают, что в каждом сеансе будет использоваться новый ключ, что обеспечит защиту от «чтения назад» – невозможность определить текущие данные обмена в будущем, после раскрытия долговременных криптографических ключей.

В дальнейшем планируется проведение исследований в области влияния и степени угрозы квантовых атак на разрабатываемую систему, возможность минимизации реализации угрозы взлома без применения постквантовых алгоритмов.

Несмотря на то что симметричные алгоритмы не являются уязвимыми для атак с применением квантовых компьютеров сами по себе, существует возможность раскрытия сеансовых ключей, с помощью атак на уязвимые асимметричные алгоритмы. Поэтому целесообразно инициировать постепенный переход на использование постквантовых алгоритмов.

Наиболее важно начинать внедрение постквантовых алгоритмов в тех областях, где информация сохраняет актуальность долгое время. Это любые пользователи и операторы конфиденциальной информации с длительным жизненным циклом:

- государственная и иная охраняемая законом тайна;
- коммерческая тайна;
- персональные данные;
- медицинские данные;
- промышленные ноу-хау.

Для других областей этот класс атак менее критичен, так как через условные десять лет информация потеряет свою актуальность. Но, скорее всего, в течение ближайших пяти – восьми лет мы увидим переход на квантово-устойчивые решения по всему миру для защиты от новых угроз. Множество систем, использующих классические асимметричные алгоритмы, могут стать уязвимыми уже в ближайшие несколько лет.

В настоящее время в США с июля 2022 года по итогам NIST (National institute of standards and technology) были отобраны несколько постквантовых алгоритмов с открытым ключом, а с ноября 2022 года был инициирован переход на постквантовую криптографию для всех внутренних агентств в течение 2023 года [4].

Литература

1. NIST [Электронный ресурс]. – 2023. – Режим доступа: <https://csrs.nist.gov/projects/post-quantum-cryptography> – Дата доступа: 05.04.2023.
2. ResearchGate [Электронный ресурс] – 2023 – Режим доступа: https://www.researchgate.net/publication/307582358_IARCCCE_An_Approach_towards_Data_Security_in_the_Cloud_Computing_Using_AES – Дата доступа: 05.04.2023.
3. PTSJ [Электронный ресурс] – 2023 – Режим доступа: <http://ptsj.ru/catalog/icec/insec/785.html> – Дата доступа: 05.04.2023.
4. Migrating to Post-Quantum Cryptography [Электронный документ]. – November 18, 2022. – Режим доступа: <https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf> – Дата доступа: 8.04.2023

КРИПТОГРАФИЧЕСКИЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ АНОНИМНОСТИ В СИСТЕМАХ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

Е.П. РЯБОВА, М.А. КАЗЛОВСКИЙ

*Белорусский государственный университет,
г. Минск, Республика Беларусь*

Введение

Голосование – это фундаментальное право человека выражать свое мнение в демократических системах. С развитием криптографических протоколов и портативных электронных устройств, таких как ноутбуки, планшеты и смартфоны, мы получили возможность голосовать дистанционно, с помощью систем электронного голосования. Многие из них были предложены в последние годы для замены бумажного голосования по ряду причин, таких как прозрачность процедуры, дешевизна проведения и увеличение явки избирателей. Однако при реализации электронного голосования необходимо выполнить ряд важных требований безопасности: анонимность, проверяемость, право голоса, прозрачность, конфиденциальность выбора. Только их соблюдение обеспечит безопасное и надежное функционирование системы электронного голосования. Целью данной работы является анализ одного из фундаментальных требований – анонимности.

1. Характеристические признаки электронного голосования

1.1. Общие этапы электронного голосования

В целом система голосования состоит из нескольких этапов в соответствии с моделью голосования. В качестве основных этапов выделяют следующие:

1. *Регистрация/Аутентификация.* Каждый избиратель должен зарегистрироваться и пройти аутентификацию перед регистрационной комиссией, чтобы подтвердить право голоса перед получением бюллетеня. Аутентификация избирателя может проводиться с помощью криптографического протокола через браузер или по электронной почте.

2. *Голосование.* Избиратель отдает свой голос, используя эксклюзивные учетные данные или ключи, предоставленные регистрационной комиссией.

3. *Подсчет голосов.* Избирательная комиссия подсчитывает все голоса и публикует результат голосования. Обычно голоса анонимны и, возможно, зашифрованы.

1.2. Требования к электронному голосованию

Для того чтобы система электронного голосования была применима на практике, она должна удовлетворять нескольким криптографическим требованиям.

Сначала мы перечислим общие требования, обязательные для большинства видов голосования, а затем приведем список дополнительных требований для противодействия атакам противника, которые характерны для дистанционного голосования.

Общие требования:

1. *Анонимность (Privacy).* Анонимность подразумевает, что связь содержимого бюллетеня избирателя и его личности должна оставаться в секрете.

2. *Проверяемость (Verifiability).*

– *индивидуальная проверяемость* означает, что избиратель может проверить свой голос, не раскрывая личность, и убедиться, что его голос учтен корректно;

– *универсальная проверяемость* предполагает, что любой желающий может проверить корректность подсчета окончательных результатов голосования.

3. *Право голоса (Eligibility).* К голосованию допускаются только включенные избирательной комиссией в списки для голосования избиратели. Обычно выполнение данного свойства реализуется с помощью аутентификации избирателя.

4. *Предотвращение множественного голосования (Multiple-voting detection)*. Будет обнаружена попытка избирателя проголосовать более одного раза, в результате чего от каждого избирателя будет учтено не более одного голоса.

5. *Конфиденциальность выбора (Fairness)*. Информация о любых промежуточных результатах голосования не может быть получена, что достигается шифрованием бюллетеней, публикуемых на этапе голосования.

Дополнительные требования:

1. *Защита от принуждения (Uncoercibility)*. Чтобы манипулировать результатами голосования, противник может использовать множество методов принуждения избирателей. Например, он может потребовать от избирателя воздержаться от голосования. Также он может представиться действительным избирателем, если получит личный ключ этого избирателя. Таким образом, система голосования должна обеспечить механизмы защиты, затрудняющие действия противника, пытающегося воздействовать на избирателя.

2. *Свобода выбора (Receipt-freeness)*. Данное требование может быть рассмотрено как частный случай защиты от принуждения. Система предполагает отсутствие возможности предоставления противнику доказательства, подтверждающего содержание голоса избирателя. Свобода выбора должна быть обеспечена даже в случае желания избирателя предъявить такое доказательство противнику.

В зависимости от целей голосования определяется необходимость выполнения описанных требования и выстраивается их приоритетность.

2. Криптографические механизмы, обеспечивающие анонимность

2.1. Перемешивание

Перемешивание – это протокол многосторонней связи, который принимает входящие сообщения, перемешивает их в случайном порядке таким образом, чтобы все стороны знали, что выполняется преобразование, и ни одна сторона при этом не знала алгоритма перестановки [1].

Перемешивание расшифрования. В этом типе перемешивания узлы имеют пару из личного и открытого ключей. Для распространения ключей используется инфраструктура открытых ключей. Пусть pub_i будет открытым ключом и $priv_i$ личным ключом для i -го узла, а r_i – случайными данными. Протокол перемешивания работает следующим образом, если избиратель отправляет сообщение v через пять узлов, предварительно зашифровав его на общем открытом ключе, полученном перемножением pub_i всех узлов:

$$v_{enc} = E_{pub_1} \left(r_1, E_{pub_2} \left(r_2, E_{pub_3} \left(r_3, E_{pub_4} \left(r_4, E_{pub_5} (r_5, v) \right) \right) \right) \right).$$

Сообщение будет последовательно зашифровано открытыми ключами всех 5 узлов, зашифрованные сообщения будут проходить через узлы в случайном порядке, а последний узел опубликует сообщение v_{enc} . Расшифрование происходит в обратном порядке с использованием личных ключей узлов [2].

Перемешивание повторного зашифрования. Используется схема шифрования с пороговым открытым ключом, которая позволяет повторно зашифровывать сообщение без знания личного ключа. Узлы совместно создают общий открытый ключ, для которого они владеют частичными личными ключами. Избиратель зашифровывает бюллетень с помощью общего открытого ключа. Каждый узел, в свою очередь, повторно зашифровывает бюллетень избирателя и переставляет бюллетени случайным образом. Его входные данные являются либо входными данными в сеть перемешивания (в случае первого узла), либо выходные данные предшествующего узла (для последующих узлов). После того как все узлы выполнили указанные операции, избирательная комиссия расшифровывает бюллетени, используя частичные личные ключи ее членов.

2.2. «Слепая» подпись

«Слепая» подпись – это один из видов цифровой подписи, при котором содержимое сообщения зашифровывается на то время, пока выполняется процесс подписи. Другими словами, данный механизм позволяет одной из сторон подписать сообщение, не имея возможности узнать его содержание. С ее помощью может быть обеспечена конфиденциальность бюллетеня избирателя: избирательная комиссия «вслепую» подписывает или эфемерный открытый ключ избирателя, или бюллетень избирателя, чтобы удостоверить их подлинность. Следовательно, регистрационная комиссия, задача которой заключается в проверке права голоса избирателя, не будет знать, как проголосует или проголосовал избиратель соответственно. При этом публикация бюллетеня обязательно должна производиться через анонимный канал связи.

Рассмотрим схему «слепой» подписи схема на основе алгоритма RSA, в основе которой лежит традиционная подпись алгоритмом RSA.

Пусть (N, e) – открытый ключ избирательной комиссии, а (N, d) – ее личный ключ, где d – обратный элемент к $e \pmod{\phi(N)}$. Избиратель выбирает случайное число r таким образом, чтобы $\text{НОД}(r, N) = 1$, и отправляет в регистрационную комиссию следующее сообщение:

$$v' = vr^e \pmod{N}.$$

Случайное число r используется для сокрытия бюллетеня v от избирательной комиссии. Регистрационная комиссия проверяет право голоса, после чего подписывает «слепой» бюллетень и отправляет обратно сообщение S' :

$$S' = (v')^d = v^d (r^e)^d = v^d r \pmod{N}.$$

После получения S' избиратель использует r для снятия «ослепления», чтобы получить обычную подпись бюллетеня S :

$$S = S' r^{-1} = v^d r r^{-1} = v^d \pmod{N}.$$

2.3. Гомоморфное шифрование

Гомоморфизм позволяет оперировать зашифрованным текстом, не расшифровывая его. Например, предположим, что существуют $E_K(m_1)$ и $E_K(m_2)$, тогда может быть получен $E_K(m_1 \odot m_2) = E_K(m_1) \odot E_K(m_2)$, где \odot может быть либо модульным сложением \oplus , либо модульным умножением \otimes .

Гомоморфизм в системах электронного голосования может быть двух видов: аддитивный гомоморфизм \oplus и мультипликативный гомоморфизм \otimes . Разница между аддитивными гомоморфными системами электронного голосования и мультипликативными гомоморфными системами электронного голосования заключается в фазе подсчета голосов. На этапе подсчета голосов для аддитивного гомоморфизма вычисляется сумма голосов за всех кандидатов: $E(m_1) \oplus E(m_2) = E(m_1 + m_2)$ [5], после чего полученная сумма расшифровывается. Для мультипликативного гомоморфизма все бюллетени перемножаются: $E(m_1) \otimes E(m_2) = E(m_1 m_2)$, произведение расшифровывается, а затем разлагается на простые множители для подсчета голосов.

2.4. Кольцевая подпись

Данный механизм обеспечивает гарантии, что некоторое сообщение было подписано одним из участников группы, при этом сохраняется анонимность личности подписанта в пределах данной группы.

Группа из r участников называется кольцом. У каждого участника i есть открытый ключ pk_i , который известен всем участникам, и личный ключ sk_i , который знает только сам участник i . Пусть $L = \{pk_1, pk_2, \dots, pk_r\}$ – список всех открытых ключей.

Механизм состоит из 2 алгоритмов:

$RingSign(M, L, sk_s) = \sigma$ – формирование подписи σ к сообщению M по открытым ключам всех участников и личному ключу подписывающего участника s ;

$RingVfy(\sigma, M, L) = 0|1$ – проверка подписи σ к сообщению M .

Связанные кольцевые подписи – это кольцевые подписи, которые обладают дополнительным свойством – связностью. Данное свойство позволяет любому участнику группы проверить, были ли созданы некоторые две кольцевые подписи одним и тем же участником группы (т.е. использовался ли для их создания один и тот же личный ключ). В случае обнаружения повторной подписи, созданной участником группы, его подписи аннулируются. Для реализации данной проверки требуется дополнительный алгоритм *Linked*. Данный алгоритм проверяет две подписи σ_1, σ_2 на действительность с помощью алгоритма *RingVfy* и связность с одним и тем же личным ключом.

3. Сравнительный анализ систем электронного голосования

Таблица 1. – Сравнительный анализ систем электронного голосования

	JCJ	PV1	PV2	ND	Cramer	Kiayias	DVLRs
Механизмы	RMN	DMN	RMN	BS	HE	HE	LRS
Сложность	$O(n^2)$	$O(n^2)$	$O(n^2)$	$O(n^2)$	$O(n)$	$O(n)$	$O(n^2)$
Анонимность	+	+	+	+	+	+	+
Индивидуальная проверяемость	+	+	+	+	–	–	+
Универсальная проверяемость	+	+	+	+	+	+	–
Право голоса	+	+	+	+	+	+	+
Множественное голосование	+	+	+	+	+	+	+
Конфиденциальность выбора	+	+	+	+	–	+	+
Защита от принуждения	+	–	–	+	–	–	–
Свобода выбора	+	+	+	+	+	–	+

Легенда: RMN – перемешивание расшифрования, DMN – перемешивание повторного зашифрования, BS – «слепая» подпись, HE – гомоморфное шифрование.

В результате сравнительного анализа была получена таблица 1, приведенная выше. Для сравнительного анализа были выбраны следующие системы электронного голосования на основе перемешивания: JCJ [3], PV1 [5], PV2 [5]; «слепой» подписи: ND [6]; гомоморфного шифрования: Cramer [7], Kiayias [8]; связанной кольцевой подписи: DVLRs [9].

Проанализировав зависимость вычислительной сложности от количества выполненных требований, приходим к выводу, что быстрдействие перпендикулярно безопасности. Однако высокая вычислительная сложность не должна являться причиной неприменимости

безопасных систем электронного голосования, так как в большинстве случаев можно разбить избирателей на отдельные группы, тем самым решив эту проблему.

Системы, основанные на перемешивании, соответствуют выдвинутым требованиям к системам электронного голосования, однако узлы перемешивания должны выполнить большую вычислительную работу, необходимую для доказательства корректности перемешивания, что является существенным недостатком.

Системы, основанные на «слепой» подписи и связываемой кольцевой подписи демонстрируют высокую эффективность, прозрачность, выполнение большого количества требований, однако для их реализации необходимо обеспечить анонимный канал связи между избирателем и избирательной комиссией.

Системы, основанные на гомоморфном шифровании, оказались наименее эффективными среди всех представленных систем электронного голосования, так как для них выполняется меньшее число требований, предъявляемых к системам электронного голосования.

Литература

1. Chaum, D.L. Untraceable electronic mail, return addresses, and digital pseudonyms / D.L. Chaum – Berkeley ; University of California, 1981. – 85 p.
2. Li H., A Taxonomy and Comparison of Remote Voting Schemes / H. Li, A.R. Kankanala, X. Zou // 23rd International Conference on Computer Communication and Networks. – 2014. – 666–672 p.
3. Juels A., Coercion-Resistant Electronic Elections / A. Juels, D. Catalano, M. Jakobsson // Towards Trustworthy Elections, New Directions in Electronic Voting. – 2010. – 37–63 p.
4. Yun-Xing Kho, Swee-Huay Heng, Ji-Jian Chin. A Review of Cryptographic Electronic Voting. – 2022.
5. Ryan P., The Prêt à Voter Verifiable Election System / P. Ryan, D. Bismark, J. Heather, S. Schneider, Z. Xia // University of Surrey. – 2010.
6. Nguyen T., Enhanced security in internet voting protocol using blind signature and dynamic ballots / T. Nguyen, T. Dang // Springer Science and Business Media New York. – 2013.
7. Cramer R., Multi-Authority Secret-Ballot Elections with Linear Work / R. Cramer, M. Franklin, B. Schoenmakers, M. Yung // CWI Report CS-R9571. – 2014.
8. Kiayias A., Self-tallying Elections and Perfect Ballot Secrecy / A. Kiayias, M. Yung // 5th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2002, Paris, France. – 2002.
9. Chen G., A new receipt-free voting scheme based on linkable ring signature for designated verifiers / G. Chen, C. Wu, W. Han, X. Chen // Embedded Software and Systems Symposia. – 2008.

О ТЕСТИРОВАНИИ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ НА ОСНОВЕ ЧАСТОТНЫХ СТАТИСТИК

М.В. МАЛЬЦЕВ, Ю.С. ХАРИН

*Научно-исследовательский институт
прикладных проблем математики и информатики
Минск, 220030, Республика Беларусь
maltsew@bsu.by, kharin@bsu.by*

Введение

Генераторы случайных и псевдослучайных числовых последовательностей (далее – генераторы) являются важнейшими элементами систем криптографической защиты информации. Последовательности, созданные генераторами, используются для формирования ключей, векторов инициализации, параметров криптографических алгоритмов и протоколов. Использование генераторов с уязвимостями снижает безопасность криптосистем, упрощает задачу злоумышленников по вычислению секретных параметров. Известным примером такой уязвимости является предсказуемость генератора в ранней версии браузера Netscape Navigator, что позволило значительно сократить время, затрачиваемое на перебор ключей шифрования [1]. Таким образом, актуальной является задача оценки качества выходных последовательностей генераторов. Для решения данной задачи широко используются методы теории вероятностей и математической статистики.

1. Математическая модель «чистой случайности»

Результатом работы стойкого генератора должна являться «чисто случайная» последовательность, математической моделью которой является равномерно-распределенная случайная последовательность (РПС) [2]. Принимающая значения из N -элементного множества A случайная последовательность $\{x_t \in A : t \in \mathbb{N}\}$, называется РПС, если для нее выполняются следующие два свойства:

1. Для любого $n \in \mathbb{N}$ и для любых $1 \leq t_1 < t_2 < \dots < t_n$ случайные величины x_{t_1}, \dots, x_{t_n} независимы в совокупности.
2. Для любого $t \in \mathbb{N}$ случайная величина x_t имеет равномерное распределение вероятностей на множестве A , т.е.

$$P\{x_t = i\} = \frac{1}{N}, i \in A.$$

Для оценки качества выходных последовательностей генераторов применяется статистическое тестирование. Статистические тесты, объединяемые в наборы (батареи), проверяют, соответствуют ли свойства наблюдаемой последовательности модели РПС. Одно из важнейших свойств РПС – равномерное распределение фрагментов длины s (s -грамм):

$$P\{x_t = i_1, \dots, x_{t+s-1} = i_s\} = \frac{1}{N^s}; i_1, \dots, i_s \in A; s = 1, 2, \dots; t = 1, 2, \dots$$

Например, в простейшем случае при $s=1$ равномерность распределения 1-грамм проверяется с помощью частотного побитового теста (frequency (monobit) test), входящего в батарею NIST [3].

2. Тестирование s -мерной равномерности

Статистические тесты, проверяющие равномерность s -мерного распределения, основаны на вычислении частот s -грамм в наблюдаемой последовательности. Существуют два подхода к вычислению данных частот: по пересекающимся или по непересекающимся фрагментам последовательности. Пусть $X_1^T = (x_1, \dots, x_T) \in A^T$ – выходная последовательность генератора длины $T = ms < \infty$, $\mathbf{1}\{B\}$ – индикаторная функция события B ($\mathbf{1}\{B\} = 1$, если B наступает, $\mathbf{1}\{B\} = 0$ в противном случае), тогда частоты s -грамм $I_1^s = (i_1, \dots, i_s) \in A^s$, вычисленные по непересекающимся фрагментам X_1^T , имеют следующий вид:

$$v(I_1^s) = \sum_{t=1}^m \mathbf{1}\{X_{(t-1)s+1}^{ts} = I_1^s\} = \sum_{t=1}^m \mathbf{1}\{x_{(t-1)s+1} = i_1, \dots, x_{ts} = i_s\}, \quad (1)$$

а частоты s -грамм I_1^s , вычисленные по пересекающимся фрагментам X_1^T , имеют вид:

$$\mu(I_1^s) = \sum_{t=1}^{T-s+1} \mathbf{1}\{X_t^{t+s-1} = I_1^s\} = \sum_{t=1}^{T-s+1} \mathbf{1}\{x_t = i_1, \dots, x_{t+s-1} = i_s\}. \quad (2)$$

Используя частоты (1) и (2), строятся статистические оценки вероятностей s -грамм $p(I_1^s) = P\{X_t^{t+s-1} = I_1^s\}$:

$$\hat{p}(I_1^s) = \frac{v(I_1^s)}{m}, \quad \hat{q}(I_1^s) = \frac{\mu(I_1^s)}{T-s+1}.$$

Если верна гипотеза $H_0 = \{X_1^T \text{ является РРСП}\}$, то частоты $v(I_1^s)$ – суммы независимых, одинаково распределенных случайных величин, математическое ожидание и ковариации которых имеют вид:

$$E\{v(I_1^s)\} = mp(I_1^s), \quad \text{cov}\{v(I_1^s), v(J_1^s)\} = mp(I_1^s)(\mathbf{1}\{I_1^s = J_1^s\} - p(J_1^s)),$$

а распределение вероятностей $\hat{p}(I_1^s)$ сходится при $m \rightarrow \infty$ к нормальному распределению с математическим ожиданием $p(I_1^s)$ и дисперсией

$$\frac{p(I_1^s)(1-p(I_1^s))}{m}.$$

Математическое ожидание оценок $\hat{q}(I_1^s)$ также, очевидно, равно $p(I_1^s)$. Кроме того, нормированные отклонения оценок

$$\bar{q}(I_1^s) = \sqrt{T-s+1}(\hat{q}(I_1^s) - p(I_1^s))$$

имеют асимптотическое нормальное распределение с нулевым математическим ожиданием и ковариационной матрицей $\Sigma = \Sigma(I_1^s, J_1^s)$ [4]:

$$\Sigma(I_1^s, J_1^s) = \frac{\sigma(I_1^s, J_1^s)}{T-s+1} + O(1/T^2),$$

Величины $\sigma(I_1^s, J_1^s)$ имеют вид [5]:

$$\sigma(I_1^s, J_1^s) = p(I_1^s)(\mathbf{1}\{I_1^s = J_1^s\} - p(J_1^s)) + p(I_1^s)S(I_1^s, J_1^s) + p(J_1^s)S(J_1^s, I_1^s), \quad (3)$$

где

$$S(I_1^s, J_1^s) = \sum_{i=1}^{\infty} (p^{(i)}(I_1^s, J_1^s) - p(J_1^s)),$$

$p^{(i)}(I_1^s, J_1^s) = \mathbf{P}\{X_{t+i}^{t+i+s-1} = J_1^s, X_t^{t+s-1} = I_1^s\}$ – вероятность перехода из состояния I_1^s в состояние J_1^s за i шагов.

В задачах тестирования генераторов $A = \{0, 1\}$; тогда, если верна гипотеза H_0 , то величины (3) принимают вид:

$$\sigma(I_1^s, J_1^s) = \frac{1}{2^s} (\mathbf{1}\{I_1^s = J_1^s\} - \frac{1}{2^s} + \sum_{i=1}^{s-1} \frac{1}{2^i} (\mathbf{1}\{I_{i+1}^s = J_1^{s-i}\} + \mathbf{1}\{J_{i+1}^s = I_1^{s-i}\}) - \frac{s-1}{2^{s-1}}).$$

Использование пересекающихся s -грамм для построения статистических тестов позволяет использовать больше информации о выходной последовательности, но требует более сложного теоретического обоснования.

3. Компьютерный эксперимент

Проиллюстрируем использование частот s -грамм, вычисляемых по пересекающимся и по непересекающимся фрагментам, при вычислении s -мерной энтропии двоичной последовательности:

$$H_s = - \sum_{I_1^s \in \{0,1\}^s} p(I_1^s) \log_2 p(I_1^s).$$

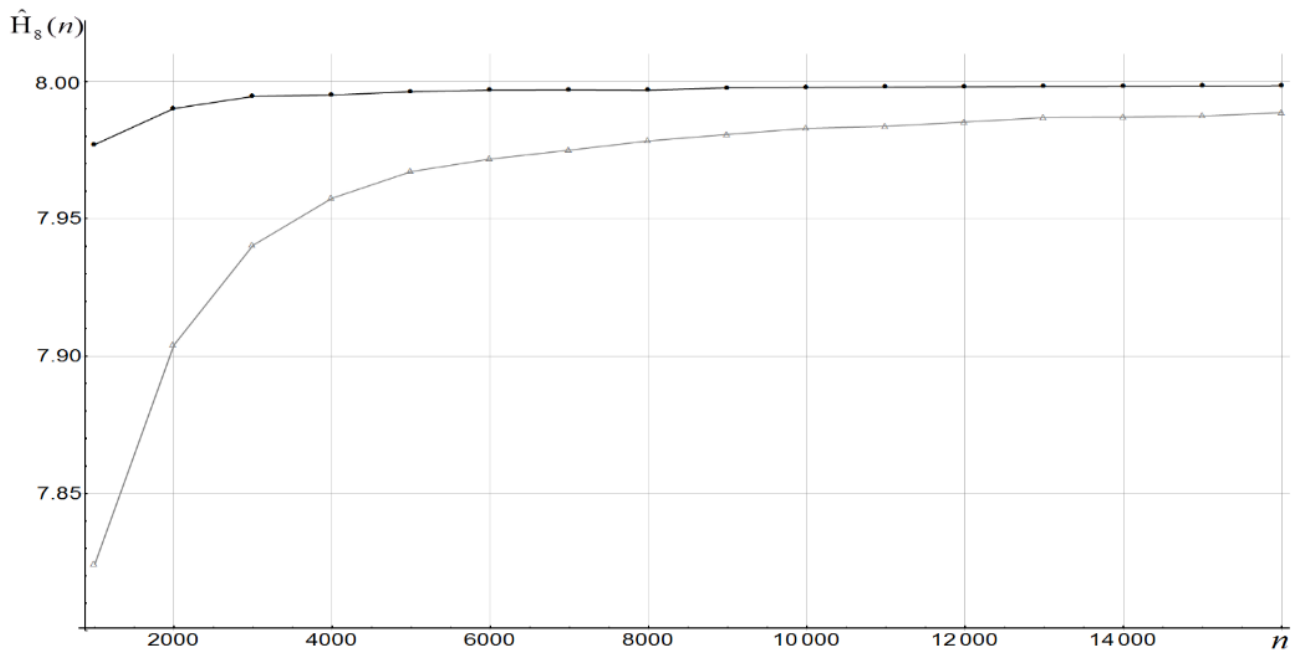


Рисунок 1. – Сравнение оценок 8-мерной энтропии, построенных по пересекающимся и по непересекающимся фрагментам двоичной последовательности

Для РРСП $H_s = s$, поэтому значимое отклонение от этой величины для выходной последовательности сигнализирует об уязвимости генератора. Рисунок 1 иллюстрирует поведение оценок энтропии $\hat{H}_s(n)$, построенных по пересекающимся (верхняя линия на графике) и непересекающимся (нижняя линия на графике) фрагментам длины 8 двоичной последовательности длины $n = 1000, 2000, \dots, 16000$, полученной с помощью алгоритма СТБ 34.101.31 (BeIT) в режиме счетчика. График иллюстрирует превосходство в точности оценок, построенных по пересекающимся фрагментам.

Литература

1. Goldberg, I. Randomness and the Netscape browser / I. Goldberg, D. Wagner // Dr. Dobb's Journal. – 1996. – Vol. 1. – P. 66–71.
2. Криптология / Ю.С.Харин [и др.]. – Минск: БГУ, 2013. – 512 с.
3. A statistical test suite for random and pseudorandom number generators for cryptographic applications [Electronic resource]: National Institute of Standards and Technology Special Publication 800-22 Rev. 1a, 2010.
4. Maltsev, M.V. On testing randomness using frequency estimators / M.V. Maltsev, Yu.S. Kharin // 13-th International Conference Computer Data Analysis and Modeling: Stochastics and data science. Minsk. 2022. – P 112–115.
5. Billingsley, P. Statistical methods in Markov chains / P. Billingsley // The Annals of Mathematical Statistics. – 1961. – Vol. 32. – P. 12–40.

НЕКОТОРЫЕ ПРОБЛЕМЫ ПОИСКА ПЭМИН ПРИ ОЦЕНКЕ ЗАЩИЩЕННОСТИ ВИДЕОИНФОРМАЦИИ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ

С.В. ХАРЧЕНКО, Д.Ю. ГАЛИЦКИЙ, В.К. ЖЕЛЕЗНЯК

*ОАО «Конструкторское бюро «Дисплей», г. Витебск, Республика Беларусь,
УО «ПГУ имени Евфросинии Полоцкой» г. Новополоцк, Республика Беларусь*

Архитектура прохождения и преобразования видеоинформации в ПК

В видеомониторах передачу информационных сигналов можно выделить по следующим путям (трактам):

ПК – Видеоконтроллер;

Видеоконтроллер – Плата драйверов матрицы.

Тракт 1 «ПК – Видеоконтроллер». К данному тракту относятся интерфейсы VGA, DVI, HDMI, DisplayPort и им подобные. Этот тракт передачи информации можно разделить на три участка:

Тракт 1.1: участок от видеоадаптера ПЭВМ до выходного видео разъема ПЭВМ. Чаще всего это дорожки на печатной плате видеоадаптера, имеющие малый размер. Также дополнительно применяются гибкие кабели-удлинители.

Тракт 1.2: участок интерфейса от выходного разъема ПЭВМ до входного видео разъема видеомонитора (внешний интерфейс VGA, DVI, HDMI и т.д.);

Тракт 1.3: участок внутри видеомонитора от входного видео разъема до видеоконтроллера (внутренний интерфейс VGA, DVI, HDMI и т.д.); Во внутреннем тракте также могут присутствовать усилители сигнала, сплиттеры, мультивьюверы и т.д.

Тракт 2 «Видеоконтроллер – Плата драйверов». К данному тракту относятся интерфейсы LVDS, V-by-One и им подобные (далее, для удобства, будем называть их все LVDS-интерфейсы).

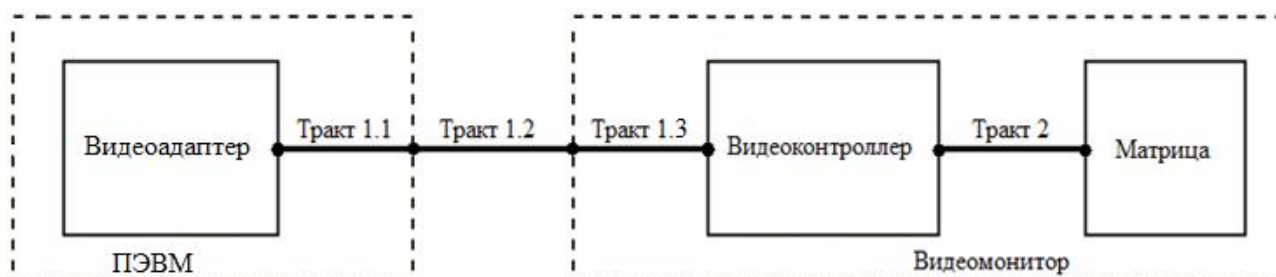


Рисунок 1. – Блок-схема прохождения видеоинформации в ПЭВМ

В исследуемых ПК интерфейсы тракта «ПЭВМ – Видеоконтроллер» служат для передачи видеоинформации от видеоадаптера системного блока до видеоконтроллера внутри видеомонитора. Видеоконтроллер – это плата расширения, обеспечивающая формирование изображения на экране монитора с использованием информации, которая передается от видеоадаптера. По средствам тракта «Видеоконтроллер – Плата драйверов матрицы» видео информация от видеоконтроллера видеомонитора передается на плату драйверов матрицы. Проанализировав теоретические данные по работе ПЭВМ, можно сделать вывод, что в зависимости от тракта передачи (используемого интерфейса) видеосигнал может иметь различные структуры, а также несколько трактов передачи, которые могут стать потенциальными каналами утечки информации. Следовательно, при оценке защищенности видеоинформации необходимо учитывать структуру видеосигнала. Также для решения проблем по ЗИ необходимо учитывать различные источники излучения (тракты передачи видеосигнала) для выдачи достоверной информации заказчику.

Результаты исследования

Исследования ПК производились путем проведения измерения электромагнитных излучений в различных частотных диапазонах. Все измерения производились с использованием аккредитованного оборудования в аттестованной полубезэховой камере в соответствии с ГОСТ Р 51320–99. В результате измерений была получена спектрограмма в частотном диапазоне 30–2000 МГц.

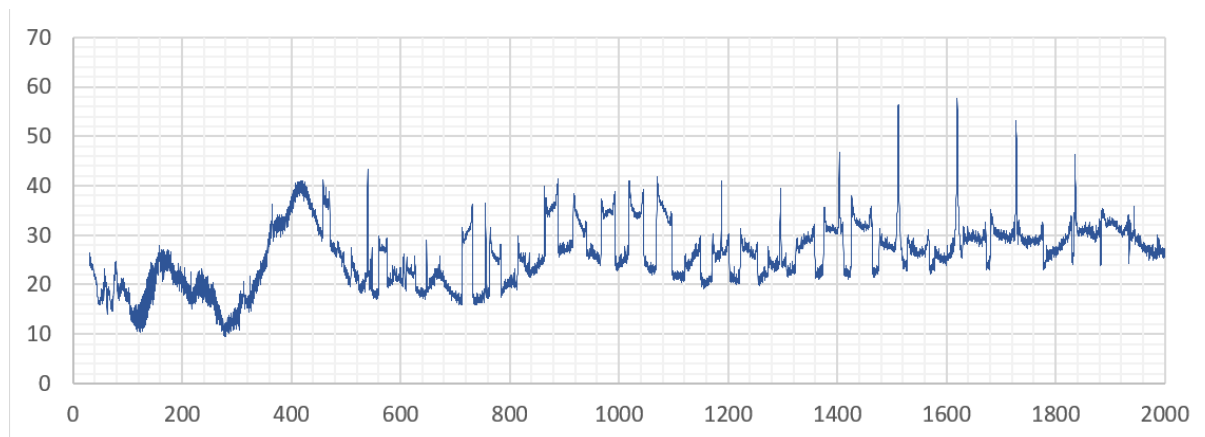


Рисунок 2. – Общий спектр излучения информационных сигналов ПК

На полученной диаграмме отчетливо выделяются два сигнала:

1 – узкополосный сигнал с тактовой частотой $F_{T1} = 53,99$ МГц;

2 – широкополосный сигнал с тактовой частотой $F_{T2} = 51,0$ МГц.

При измерениях ПЭМИН и расчетах минимальных радиусов контролируемых зон, появляется проблема по поиску и разделению спектров сигналов от разных трактов.

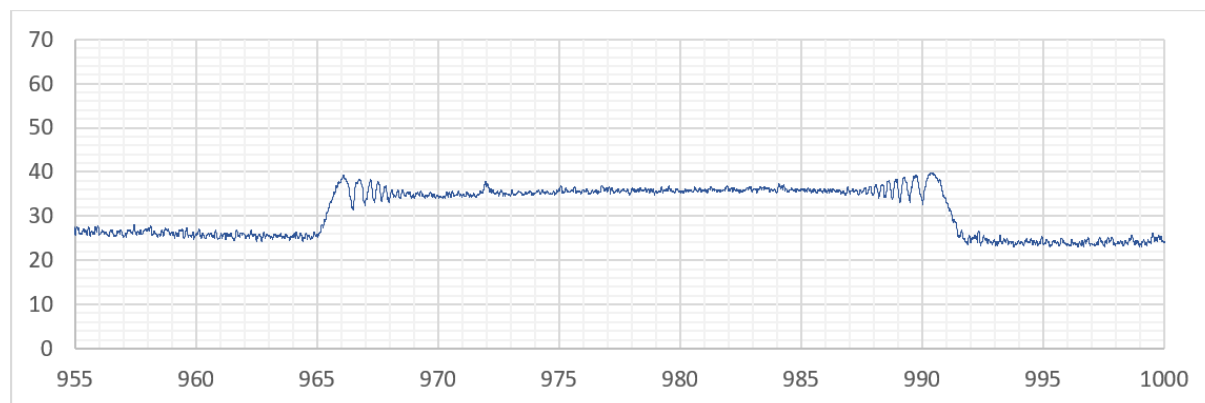


Рисунок 3. – Маскирование узкополосного сигнала DVI широкополосным сигналом LVDS

Некоторые гармонические составляющие сигнала DVI маскируются широкополосными составляющими сигнала LVDS.

Для распознавания скрытых сигналов можно использовать следующие методы.

1. Измерение двух спектров излучаемых сигналов с последующим наложением одного на другой. При измерении первого спектра включается тестовый сигнал (для соответствующего интерфейса), но отключается питание видеоконтроллера. Измерение второго спектра производится с тем же тестом, но включенным видеоконтроллером. В результате наложения одного спектра на другой отчетливо видно замаскированный сигнал.

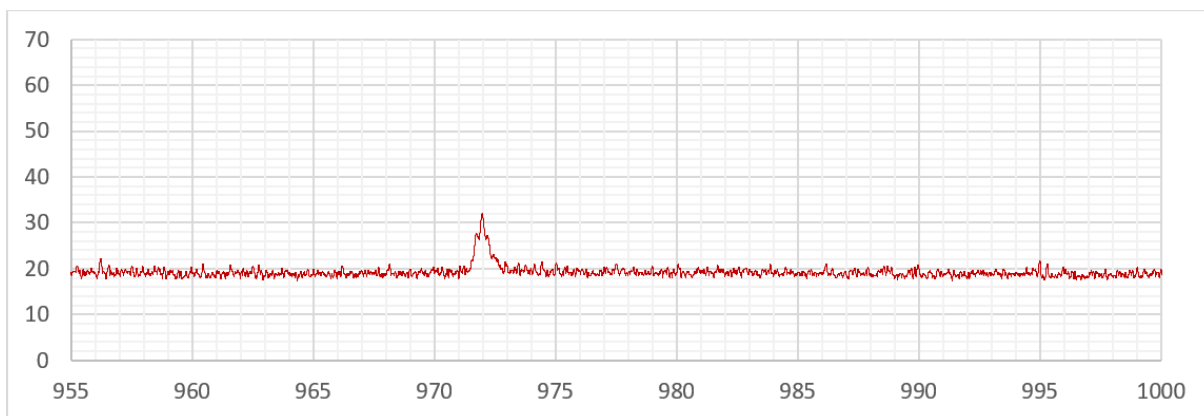


Рисунок 4. – Спектрограмма фоновой обстановки с сигналом DVI и выключенным видеоконтроллером

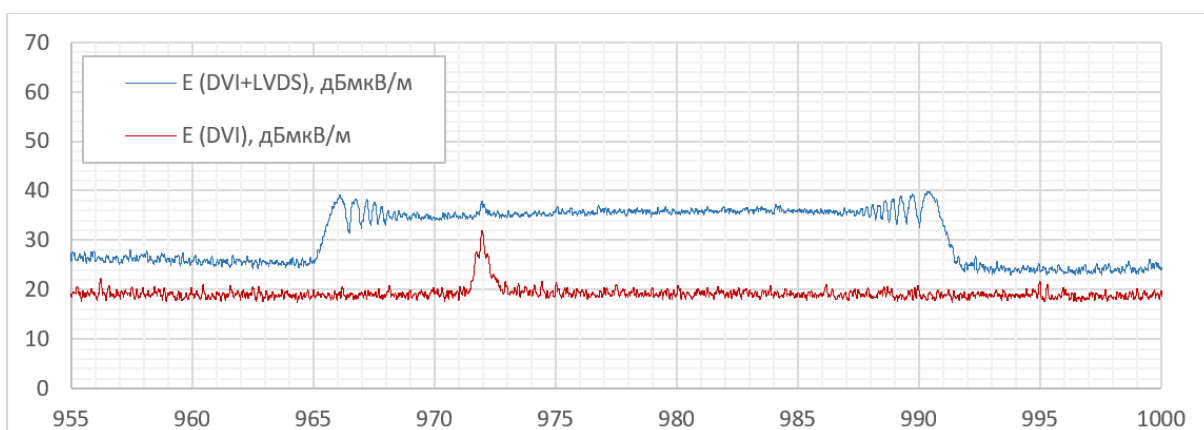


Рисунок 5. – Наложение спектрограмм с выключенным и включенным видеоконтроллером

2. Использование для измерений приемников с функцией анализа спектра в реальном времени (Real-Time Spectrum Analyzers или RTSA). Из-за непостоянства частоты LVDS-сигнала данный сигнал размывается. Использование функции анализа спектра в реальном времени позволяет различить на спектрограмме широкополосные (в нашем случае LVDS) и узкополосные (DVI) сигналы даже в случае их наложения

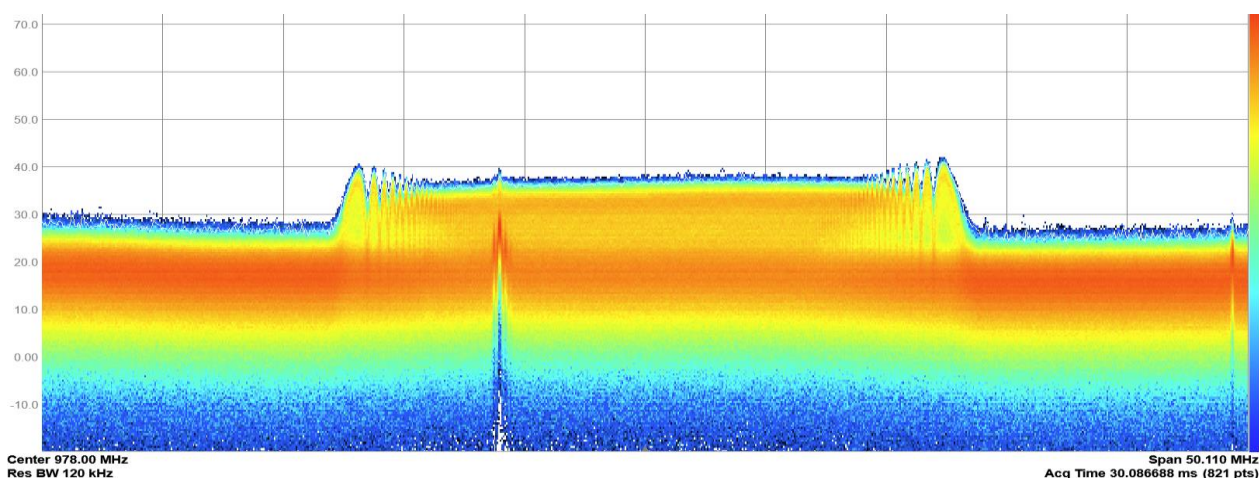


Рисунок 6. – Спектрограмма полученная при помощи функции анализа спектра в реальном времени

Заключение

В результате проведения исследований удалось выявить проблему маскирования одного информационного видеосигнала другим. Для решения данной проблемы предложены методы, коррелирующие между собой, что подтверждает их эффективность. При разработке методик оценки защищенность видеoinформации необходимо учитывать выявленную проблему.

Литература

1. Железняк В.К. Защита информации от утечки по техническим каналам: учебное пособие. – ГУАП. – СПб, 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. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. – 436 с.

МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ВЫРАБОТКЕ ОБЛАЧНОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

В.А. ГЕРАСИМОВ¹, М.А. КАЗЛОВСКИЙ¹, О.В. БОЙПРАВ²

¹Научно-производственное республиканское унитарное предприятие
«Научно-исследовательский институт технической защиты информации»,
²Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Введение

Электронная цифровая подпись предназначена для контроля целостности и подлинности электронных документов. При выработке подписи используется личный ключ, который находится в распоряжении владельца. Только владелец личного ключа может выработать корректную подпись. Корректность подписи означает, что документ не был изменен и не позволяет владельцу отказаться от авторства подписанного документа [1].

В настоящее время процесс выработки электронной цифровой подписи может быть реализован в формате облачного сервиса. Такой сервис позволит обеспечить удобные и безопасные условия использования электронной цифровой подписи как для физических, так и для юридических лиц. При использовании этого сервиса подписант передает личный ключ в защищенное облачное хранилище. Тем не менее владелец не теряет контроль над своим ключом, так как выработка подписи происходит только после успешной аутентификации и явной передачи права подписать определенный документ системе документооборота.

Для безопасной выработки облачной электронной цифровой подписи можно предложить систему облачной подписи (далее – СОП), в которую входят [2] следующие компоненты:

- сервер подписи (далее – СП), предназначенный для генерации и хранения личных ключей подписантов, выработки ЭЦП под контролем подписантов от их лица, при этом составным компонентом СП является аппаратное устройство создания подписи (далее – УСП);
- сервер документооборота (далее – СД), предназначенный для создания и проверки электронного документа;
- клиентская программа (далее – КП), предназначенная для взаимодействия подписанта с компонентами системы облачной подписи;
- сервер регистрации (далее – СР), отвечающий за регистрацию и деактивацию аккаунтов подписантов в СОП;
- прикладная система (далее – ПС), внешний компонент по отношению к системе облачной подписи, отвечающий за загрузку, разработку, хранение и отображение подписываемых документов.

Однако, распределения обязанностей между компонентами не может являться гарантией безопасности СОП. Для того чтобы СОП гарантировала корректное использование личного ключа подписанта авторы предлагают использовать определенные механизмы, которые позволят обеспечить прозрачное и безопасное функционирование СОП.

1. Использование JWT при аутентификации пользователей

Для обеспечения надежной передачи данных между компонентами СОП используется JSON Web Token (далее – JWT). Объект JWT состоит из нескольких кодовых слов, разделенных символом «.» (точка), которые описывают компоненты, представляющие собой объекты в формате JSON. Компоненты сначала кодируются по правилам UTF8, а затем по правилам base64url [3].

Для обеспечения принципов целостности и подлинности информации используется модифицированный объект JSON Web Signature (далее – JWS), который представляет собой один из типов JWT.

Объект JWS состоит из трех компонентов: заголовок, подписываемые данные и подпись. Предложенная модификация состоит в том, что третья часть JWS представляет собой не подпись, а CMS-структуру с отсоединенными данными, которая помимо подписи содержит дополнительные атрибуты. Это сделано для того, чтобы упростить проверку JWS с помощью входящих в состав CMS-структуры атрибутов.

2. Использование сетевого токена для аутентификации пользователей

Аутентификация подписанта в КП проходит после аутентификации в ПС. Для связи сеанса ПС с КП используется сетевой токен, который генерируется СП в соответствии с требованиями СТБ 34.101.47-2017 «Информационные технологии и безопасность. Алгоритмы генерации псевдослучайных чисел» с применением режима TOTP (A.8), длиной 6 символов.

Сетевой токен относится к фактору «чем я владею». Вместе с сетевым токеном, который подписант получает по каналу GSM, аутентификация проводится и по коду сессии. Для получения кода сессии вычисляется хеш-значение от описанного в пункте 1 модифицированного JWS. Восемь последних шестнадцатеричных символов полученного хеш-значения являются кодом сессии.

3. Использование PIN для аутентификации пользователей

Для подписи документа пользователь должен ввести PIN-код, который позволит получить доступ к личному ключу. PIN-код относится к фактору «что я знаю». PIN-код должен состоять как минимум из 6 символов. Дополнительно PIN-код используется для парольной аутентификации сторон и формирования общего ключа защищенного соединения между КП и УСП с использованием криптографического протокола VPАСЕ, определенного в СТБ 34.101.66-2014 «Информационные технологии и безопасность. Протоколы формирования общего ключа на основе эллиптических кривых».

4. Использование данных активации подписи для повышения уровня гарантий контроля

При выработке облачной электронной цифровой подписи определяются уровни гарантий контроля (далее – УГК). Для системы облачной подписи определяются два УГК: УГК1 (базовые гарантии) и УГК2 (высокие гарантии).

УГК1 может применяться только тогда, когда компрометация личного ключа приводит к минимальным потерям. Например, этот уровень соответствует ситуации, когда подписываются документы, предназначенные для использования только внутри организации для ее собственных нужд.

УГК2 может применяться для подписи юридически значимых документов. При применении УГК2 является обязательным применение данных активации подписи (далее – ДАП). ДАП являются результатом криптографических преобразований, которые связывают, аутентификацию подписанта, идентификатор личного ключа подписанта и данные для подписи. Формирование ДАП независимо друг от друга выполняют КП и УСП. При совпадении ДАП, переданных от КП в УСП, с ДАП, сформированными в УСП, УСП выполняет выработку значения электронной цифровой подписи.

5. Использование протокола активации подписи для повышения уровня гарантий контроля

Для повышения гарантий контроля при выработке электронной цифровой подписи вводится понятие протокола активации подписи (далее – ПАП). Он представляет собой последовательность действий, которую должны выполнить компоненты СОП для получения электронной цифровой подписи документа.

Основные обозначения, используемые в алгоритме ПАП, представлены в таблице 1.

Таблица 1. – Список основных обозначений алгоритма ПАП

Обозначение	Пояснение
$A \rightarrow B$	Обмен информацией между сторонами от А к В
JWS – M	Передача данных в формате JSON Web Signature Mode
JSON(<i>data1, data2, ..., dataN</i>)	Передача данных в формате JavaScript Object Notation
$h(data)$	Хэш-значения данных, выработанные по алгоритму из СТБ 34.101.31-2020 (пункт 7.8)
$val1 val2 \dots valn$	Конкатенация значений
$display(Source: data1, data2, \dots, dataN)$	Отображение в клиенте определенных данных Пример: $display(КП: CodeSession, OTP),$ $display(ПС: hDoc, IdSession)$
$input(data1, data2, \dots, dataN)$	Ввод значений через устройство ввода (выбор документа через диалоговые окна, ввод PIN или OTP, CodeSession). Пример: $input(КП: CodeSession, OTP),$ $input(ПС: CodeSession, OTP)$ В примере пользователь через КП и ПС заполняет данные о CodeSession и OTP
$formation(data1, data2, \dots, dataN) \rightarrow JWS - M(JWSname)$	Формирование JWS-M из данных и запись под ключом JWSname
$auth(source)$	Прохождение аутентификации
$save(data1, data2, \dots, dataN)$	Сохранение данных
<i>and, or</i>	Варианты и/или
[<i>data</i>]	Массив, состоящий из элементов <i>data</i>
ASNdata	Подписанные данные, возвращенные СД
Attr	Атрибуты, которые извлекаются из ASNdata
AuthData	Подтверждение аутентификации пользователя
CMS	Структура, которая передается в качестве результата выполнения протокола активации подписи
CodeSession	Код сессии
Count	Количество данных (числовой тип);
Doc	Номер текущего документа
hData	Хэш-значение подписываемых данных
hDoc	Хэш-значение документа
IdSession	Идентификатор сессии
IdSlot	Идентификатор слота
Message	Информационное сообщение
NumberPhone	Номер мобильного телефона, указанный в данных подтверждения аутентификации
OTP	Одноразовый пароль
SignVal	Значение подписи
SlotList	Список слотов, содержащий информацию о слотах пользователя
Status	Статус выполнения операции (true/false)
ЕС ИФЮЛ	Единая система идентификации физических и юридических лиц
СОК	Сертификат открытого ключа

Сам алгоритм протокола активации подписи имеет вид:

1. auth(ПС: ЕС ИФЮЛ)(строгая аут.) or auth(ПС: ПС) (базовая аут.)
2. formation($hDoc, NumberPhone, IdNum, count, \dots, etc$) \rightarrow
 $JWS - M(AuthData)$ and ПС \xrightarrow{TLS} СД: JSON($AuthData$)
3. СД \xrightarrow{TLS} ПС: JSON($IdSession, CodeSession$)
4. display(ПС: $CodeSession, hDoc[1], hDoc[2], \dots, hDoc[n]$)
5. СД \xrightarrow{TLS} СП: JSON($IdSession, AuthData$)
6. СП \xrightarrow{TLS} ОТП: JSON($NumberPhone$)
7. input(КП: $CodeSession, OTP$)
8. КП \xrightarrow{TLS} СП: JSON($CodeSession, OTP$)
9. СП \xrightarrow{TLS} КП: JSON($IdSession, SlotList$)
10. display(КП: $SlotList$)
11. input(КП: $IdSlot, IdSession$)
12. КП \xrightarrow{TLS} СП: JSON($IdSlot, IdSession$)
13. СП \xrightarrow{TLS} СД: JSON($IdSession, COK$)
14. СД \xrightarrow{TLS} СП: JSON($IdSession, \{hDoc[1], hData[1], ASNdata[1]\},$
 $\{hDoc[2], hData[2], ASNdata[2]\}, \dots, \{hDoc[n], hData[n], ASNdata[n]\}$)
15. save(СП: $\{\{hDoc[1], hData[1], ASNdata[1]\}, \{hDoc[2], hData[2], ASNdata[2]\}, \dots,$
 $\{hDoc[n], hData[n], ASNdata[n]\}$)
16. КП \xrightarrow{TLS} СП: JSON($IdSession$)
17. СП \xrightarrow{TLS} КП: JSON($IdSession, count, \{\{hDoc[1], ASNdata[1]\}, \{hDoc[2], ASNdata[2]\}, \dots,$
 $\{hDoc[n], ASNdata[n]\}$)
18. display(КП: $hDoc[i], attr[i]$) and КП \xrightarrow{TLS} СП: JSON($IdSession, hData, Doc[i]$)
19. СП \xrightarrow{TLS} КП: JSON($IdSession, hData, Status$)
20. КП $\xrightarrow{TLS+BPACE(user)}$ УСП: DAP
21. save(УСП: ДАП)
22. КП \xrightarrow{TLS} СП: $IdSession, hData, IdSlot$
23. СП $\xrightarrow{BPACE(own)}$ УСП: $IdSession, hData, idslot$
24. УСП $\xrightarrow{BPACE(own)}$ СП: SignVal
25. СП \xrightarrow{TLS} СД: JSON($IdSession, SignVal, hData$)
26. save(СД: SignVal) and СД \xrightarrow{TLS} СП: JSON($Status$)
27. СП \xrightarrow{TLS} КП: JSON($Status$)
28. display(КП: message)
29. ПС \xrightarrow{TLS} СД: JSON($IdSession$)
30. СД \xrightarrow{TLS} ПС: JSON($[CMS]$)
31. display(ПС: CMS)

Заключение

Таким образом, предложенные механизмы обеспечивают достаточный уровень гарантий контроля пользователем личного ключа подписанта, используемого в СОП. Реализация данных механизмов позволяет снизить уровень риска неавторизованной выработки электронной цифровой подписи от лица пользователя и достигнуть соответствия требованиям проекта стандарта «Информационные технологии и безопасность. Требования безопасности к системам облачной подписи».

Литература

1. СТБ 34.101.45-2013 Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых. [Электронный ресурс] – Режим доступа: <https://apmi.bsu.by/resources/std.html>. – Дата доступа: 07.04.2023.

2. СТБ 34.101.bclo Информационные технологии и безопасность. Требования безопасности к системам облачной подписи. [Электронный ресурс] – Режим доступа: <https://apmi.bsu.by/resources/std.html>. – Дата доступа: 07.04.2023.

3. СТБ 34.101.87-2022 Информационные технологии и безопасность. Инфраструктуры аутентификации. [Электронный ресурс] – Режим доступа: <https://apmi.bsu.by/resources/std.html>. – Дата доступа: 07.04.2023.

ПОГЛОТИТЕЛИ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ С ГЕОМЕТРИЧЕСКИМИ НЕОДНОРОДНОСТЯМИ ПОЛУСФЕРИЧЕСКОЙ ФОРМЫ

Е.С. БЕЛОУСОВА, О.В. БОЙПРАВ,
Д.В. БОРДИЛОВСКАЯ, С.В. САВАНОВИЧ

*Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь*

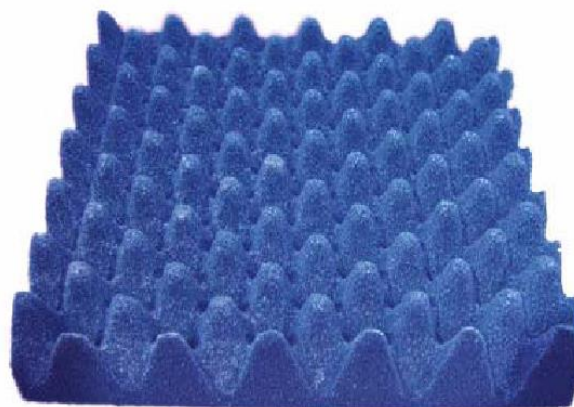
Введение

В области разработки и совершенствования радиопоглощающих материалов и конструкций экранов электромагнитного излучения широко используются различного вида геометрические неоднородности, состоящие из плоских, трубчатых, клинообразных, пирамидальных элементов. Давно известно [1], что уменьшение отражения электромагнитной волны от наружной поверхности радиопоглощающего покрытия обеспечивается ее рельефностью, шероховатостью, наличием дефектов. Так при использовании пирамидальных элементов число отражений электромагнитной волны от их поверхности зависит от высоты и величины угла каждого элемента. В случае, если элементы имеют пористую форму, то величина и распределение пор способствуют уменьшению коэффициента отражения и обеспечивают уменьшение мощности электромагнитной волны.

В качестве примера конструкций экрана с пирамидальными структурами на основе иглопробивного углеродосодержащего материала можно рассмотреть конструкцию, представленную на рисунке 1 *а* [2]. Такая конструкция характеризуется значениями коэффициента отражения порядка $-16...-18$ дБ и коэффициент передачи -10 дБ в диапазоне 6–12 ГГц.



а



б

Рисунок 1. – Внешний вид конструкции экрана электромагнитного излучения с пирамидальными структурами (*а*) и широкополосного поглотителя с волокнообразной поверхностью (*б*)

Другим примером является широкополосный поглотитель (рис. 1 *б*), выполненный из гибкой уретановой пены с волокнообразной поверхностью, обработанный огнестойким диэлектрическим материалом [3]. Отражающая способность такого поглотителя достигает 40 дБ в диапазоне частот 6–15 ГГц. Данные примеры показывают, что плавность рельефа поверхности материала может способствовать уменьшению коэффициента отражения электромагнитного излучения. Необходимо отметить, что недостатком данных материалов является их быстрый износ при длительной эксплуатации, которых может привести

к физической деформации поверхности, а следовательно искажению показателей коэффициентов отражения и передачи. Авторами предложены использовать для изготовления поглотителей электромагнитного излучения с геометрически неоднородной поверхностью двухкомпонентную полиуретановую мастику с добавлением порошкообразного углерода для увеличения износостойкости и срока службы таких материалов [4].

В данной работе представлены результаты исследования влияния расстояния между геометрическими неоднородностями полусферической формы углесодержащих поглотителей электромагнитного излучения на частотные характеристики коэффициентов отражения и передачи.

1. Методика проведения эксперимента

На рисунке 2 представлен образец углесодержащего поглотителя электромагнитного излучения с рядами геометрических неоднородностей полусферической формы, расположенными на расстоянии 2 мм. В качестве углесодержащей добавки в двухкомпонентную полиуретановую мастику использовался порошкообразный активированный березовый уголь.



Рисунок 2. – Внешний вид углесодержащего поглотителя электромагнитного излучения с геометрическими неоднородностями полусферической формы

Измерения коэффициентов отражения и передачи производились на панорамном измерителе коэффициентов передачи и отражения SNA 0,01–18, обеспечивающем выделение и определение уровней падающей и отраженной волн в диапазоне частот 2–17 ГГц. Измерения коэффициентов отражения осуществлялось в режиме согласованной нагрузки (СН) и короткого замыкания (КЗ) при вертикальной и горизонтальной ориентации рядов неоднородностей полусферической формы и расстоянии между рядами 2 мм и 20 мм.

2. Результаты и их обсуждение

На рисунке 3 представлены частотные характеристики коэффициентов отражения и передачи для образцов углесодержащего поглотителя электромагнитного излучения с геометрическими неоднородностями полусферической формы, расположенными в ряды, расстояние между которыми составляло 2 мм (кривая 1) и 20 мм с вертикальной (кривая 2) и горизонтальной ориентацией (кривая 3).

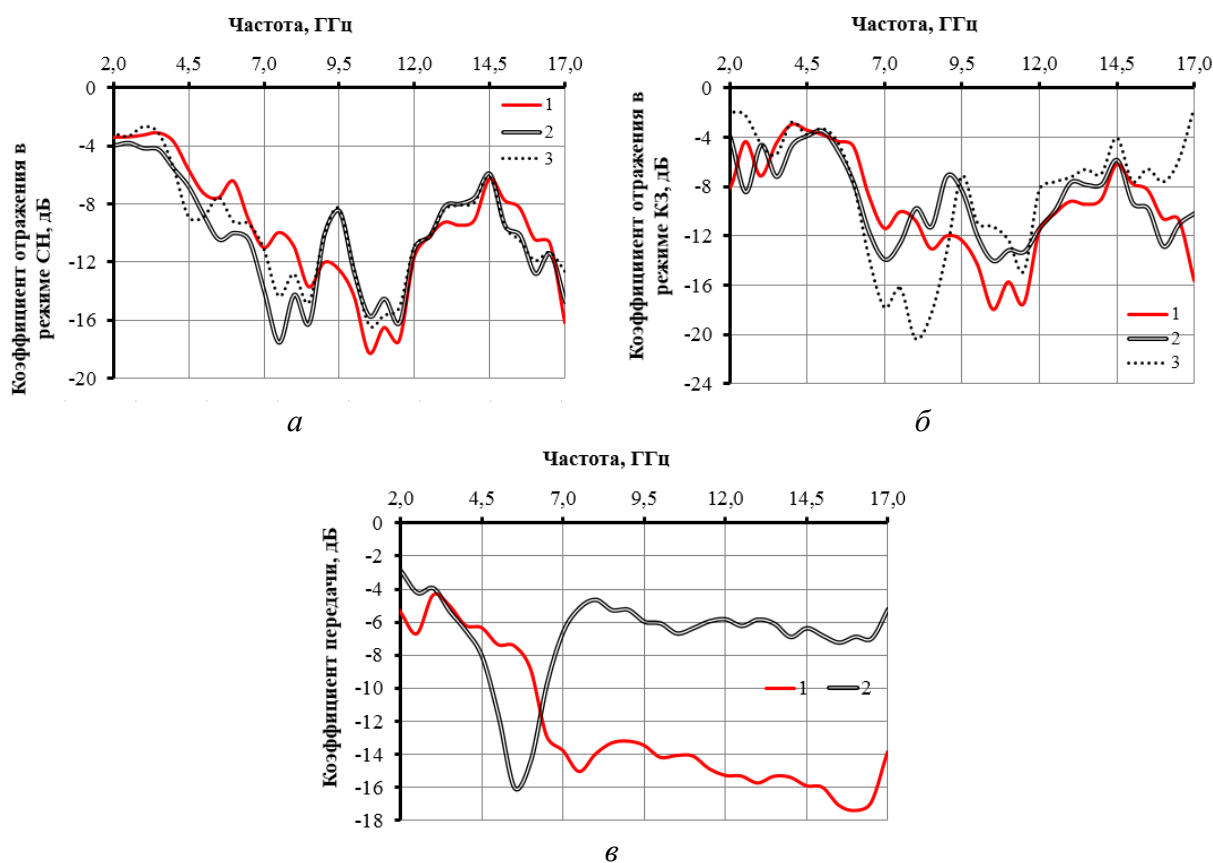


Рисунок 3. – Частотные характеристики коэффициентов передачи и отражения, измеренных в режиме СН и КЗ

Как видно из рисунка 3 *а*, минимальные значения коэффициентов отражения в режиме СН получены для образца углесодержащего поглотителя электромагнитного излучения с геометрическими неоднородностями полусферической формы, расположенными в ряд на расстоянии 2 мм (–17,6 дБ на частоте 7,5 ГГц; –16,2 дБ на частоте 8,5 ГГц) и на расстоянии 20 мм с вертикальной ориентацией (–18,3 дБ на частоте 10,5 ГГц; –17,4 дБ на частоте 11,5 ГГц). При горизонтальном расположении образца углесодержащего поглотителя электромагнитного излучения с геометрическими неоднородностями полусферической формы на расстоянии 20 мм с учетом погрешности значение коэффициента отражения в режиме СН коррелирует со значениями коэффициентов отражения при расположении геометрических неоднородностей на расстоянии 2 мм.

На частоте 8 ГГц минимальные значения коэффициента отражения в режиме КЗ (–17,8 дБ на частоте 7 ГГц; –20,3 дБ на частоте 8 ГГц) получено при вертикальной ориентации образца углесодержащего поглотителя электромагнитного излучения с геометрическими неоднородностями полусферической формы, расположенными в ряд на расстоянии 20 мм. Если расположение между неоднородностями будет минимальным, то минимумы (–17 дБ; –18,5 дБ) коэффициента отражения в режиме короткого замыкания будет зафиксирован на частотах 10,5 ГГц, 11,5 ГГц.

Как следует из рисунка 3, *в*, коэффициент передачи для образца углесодержащего поглотителя электромагнитного излучения с геометрическими неоднородностями полусферической формы составляет менее –12 дБ на частотах больше 7,5 ГГц, что на 8–10 дБ меньше, чем у образца с большим расстоянием между однородностями.

Заключение

1. Углесодержащие поглотители электромагнитного излучения с геометрическими неоднородностями полусферической формы, расположенные на минимальном расстоянии друг от друга характеризуются значениями коэффициентов отражения и передачи менее –

10 дБ на частотах больше 7 ГГц, что позволяет рекомендовать их использование для защиты радиоэлектронного оборудования от электромагнитных помех.

2. Увеличение расстояния между рядами геометрических неоднородностей полусферической формы углесодержащих поглотителей электромагнитного излучения способствует смещению минимумов частотных характеристик коэффициентов отражения в частотном диапазоне на 2–3 ГГц.

3. Экспериментально показано, что вертикальная ориентация рядов геометрических неоднородностей полусферической формы и их расположение на расстоянии 20 мм обеспечивает уменьшение коэффициента отражения до –21 дБ на частотах 7–9 ГГц.

Литература

1. Михайлин, Ю.А. Волокнистые полимерные композиционные материалы в технике / Ю.А. Михайлин. – Санкт-Петербург: НОТ, 2013. – 720 с.

2. Электромагнитные экраны на основе алюминия, его оксидов и углеродных волокон. Технологии, конструкции и свойства / Абдулхади Хаисам Дия Абдулхади [и др.]. – Минск: Бестпринт, 2021. – 120 с.

3. Техническое описание C-RAM FAC, высокопроизводительный волнистый материал // ЭлекТрейд-М [Электронный ресурс]. – 2023. – Режим доступа: http://www.eltm.ru/editor/upload-files/C-RAM_FAC__390-7_.pdf

4. Способ изготовления углесодержащего поглотителя электромагнитного излучения с геометрически неоднородной поверхностью и углесодержащий поглотитель электромагнитного излучения с геометрически неоднородной поверхностью, изготовленный этим способом: заявка на изобрет. № 20220116 / С.Э. Саванович, Е.С. Белоусова, О.В. Бойправ. – Заявл. 29.04.2022.

ФОРМИРОВАНИЕ КАНАЛОВ УТЕЧКИ РЕЧЕВЫХ СИГНАЛОВ ПРИ ОТСЧЕТНО-ДИСКРЕТНОМ ПРЕОБРАЗОВАНИИ

В.К. ЖЕЛЕЗНЯК, С.В. ЛАВРОВ,
А.Г. ФИЛИППОВИЧ, М.М. БАРАНОВСКИЙ

*Учреждение образования «Полоцкий государственный университет
имени Евфросинии Полоцкой», г. Новополоцк, Республика Беларусь*

*Оперативно-аналитический центр при Президенте Республики Беларусь,
г. Минск, Республика Беларусь*

В работе [1] исследовано, что для реализации высоких требований по передаче с высокой точностью речевой информации установлены методы ее защиты в каналах утечки речевых сигналов. Амплитудная характеристика квантователя при аналого-дискретном преобразовании речи является ступенчатой функцией и представляется в виде суммы идеальной линейной и нелинейной характеристик, последняя из которых формирует искажение сигнала [2]. Характеристикой искажений является последовательность импульсов пилообразной формы. Преобразованием Фурье эта последовательность раскладывается на спектральные составляющие четной и нечетной последовательностей $k = 1, 2, 3, 4, 5 \dots$. В работе [3] показана деформация косинусоидального колебания и периодической последовательности импульсов пилообразной формы при квантовании.

Академик В.А. Котельников положил начало развитию теории статистических оптимальных систем. Решена задача обнаружения сигналов, зависимых от конечного числа неизвестных параметров в присутствии случайных помех. Методы статистических испытаний определяют методами решения математических задач и задач исследования сложных систем при помощи моделирования сложных реализаций и имитаций случайных процессов с оценкой их вероятностных характеристик.

Ряд Котельникова записывается как

$$f(t) = \sum_{k=1}^{\infty} f(k\Delta t) \frac{\sin 2\pi F(t - k\Delta t)}{2\pi F(t - k\Delta t)}. \quad (1)$$

Полученное выражение представляет собой разложение непрерывной функции $f(t)$ в ряд по ортогональным функциям вида $\frac{\sin x}{x}$.

Разложим периодическую стробирующую функцию, показанную на рисунке 1, в экспоненциальный ряд Фурье и изобразим ее частотный спектр.

Стробирующая функция имеет ширину (длительность импульса) t_u и период повторения T , с.

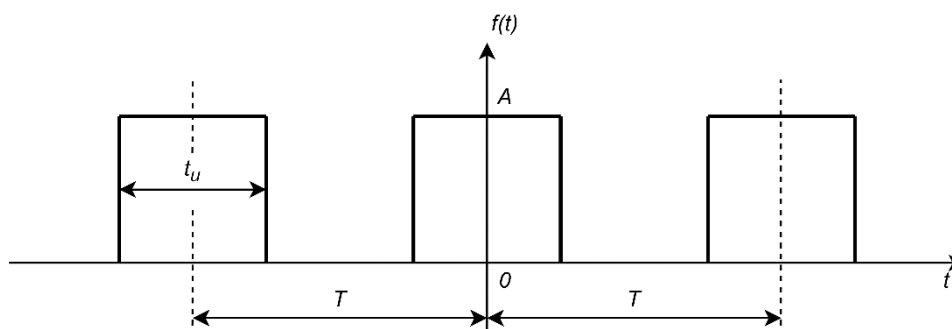


Рисунок 1. – Периодическая стробирующая функция

На интервале в один период функцию можно аналитически записать как

$$f(t) = \begin{cases} A & \text{при } \left(-\frac{t_{\text{и}}}{2} < t < \frac{t_{\text{и}}}{2}\right), \\ 0 & \text{при } \left(\frac{t_{\text{и}}}{2} < t < T - \frac{t_{\text{и}}}{2}\right). \end{cases}$$

Для удобства выберем пределы интегрирования от $-\frac{t_{\text{и}}}{2}$ до $T - \frac{t_{\text{и}}}{2}$:

$$\begin{aligned} F_n &= \frac{1}{T} \int_{-\frac{t_{\text{и}}}{2}}^{T - \frac{t_{\text{и}}}{2}} f(t) e^{-i n \omega_0 t} dt = \frac{1}{T} \int_{-\frac{t_{\text{и}}}{2}}^{T - \frac{t_{\text{и}}}{2}} A e^{-i n \omega_0 t} dt = \frac{-A}{-i n \omega_0 T} e^{-i n \omega_0 t} \Bigg|_{-\frac{t_{\text{и}}}{2}}^{T - \frac{t_{\text{и}}}{2}} = \\ &= \frac{2A}{n \omega_0 T} \sin\left(\frac{n \omega_0 t_{\text{и}}}{2}\right) = \frac{A t_{\text{и}}}{T} \left[\frac{\sin\left(\frac{n \omega_0 t_{\text{и}}}{2}\right)}{\frac{n \omega_0 t_{\text{и}}}{2}} \right]. \end{aligned} \quad (2)$$

Заключенная в скобки функция имеет форму $\frac{\sin x}{x}$ и называется функцией отсчетов.

В дальнейшем эта функция обозначается как

$$Sa(x) = \frac{\sin x}{x}. \quad (3)$$

Функция отсчетов показана на рисунке 2.

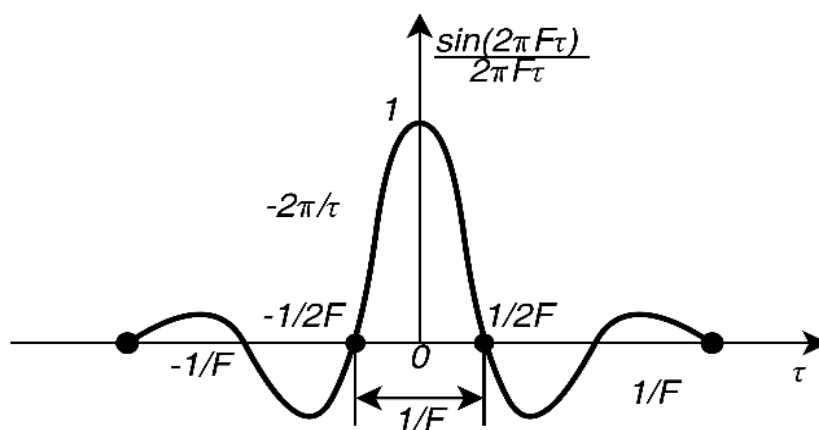


Рисунок 2. – Функция отсчетов $Sa(x)$

Заметим, что она осциллирует с периодом 2π , спадая по амплитуде с увеличением x и переходя через нуль в точках $x = \pm\pi, \pm 2\pi, \pm 3\pi$ и т.д. Из формулы (2) следует, что

$$F_n = \frac{A t_{\text{и}}}{T} Sa\left(\frac{n \omega_0 t_{\text{и}}}{2}\right).$$

Поскольку $\omega_0 = \frac{2\pi}{T}$, $\frac{n\omega_0 t_{\text{н}}}{2} = \frac{n\pi t_{\text{н}}}{T}$, получаем

$$F_n = \frac{At_{\text{н}}}{T} \text{Sa}\left(\frac{n\pi t_{\text{н}}}{T}\right), \quad (4)$$

$$f(t) = \frac{At_{\text{н}}}{T} \sum_{n=-\infty}^{\infty} \text{Sa}\left(\frac{n\pi t_{\text{н}}}{T}\right) e^{i n \omega_0 t}. \quad (5)$$

Из формул (4), (5) следует, что F_n – действительная величина, поэтому для частного представления достаточно одного спектра.

Величины $f(k\Delta t)$ называются отсчетами функции $f(t)$. Они определяют значения исходной функции $f(t)$ в дискретные моменты времени $k\Delta t$. Множитель $\frac{\sin 2\pi F(t - k\Delta t)}{2\pi F(t - k\Delta t)}$ называется функцией отсчетов.

Если обозначить $\tau = t - k\Delta t$, то функция отсчетов примет вид:

$$\psi[\tau] = \frac{\sin 2\pi F \tau}{2\pi F \tau}. \quad (6)$$

Функция отсчетов принимает наибольшее значение, равное единице, в моменты времени $t = k\Delta t$ ($\tau = 0$) и обращается в нуль в моменты времени $t = (k \pm m)\Delta t$, где $m = 1, 2, 3 \dots$. Ширина главного лепестка функции отсчетов на нулевом уровне равна $1/F$. Спектр функции отсчетов является равномерным в полосе $(-F, F)$ и равен нулю вне этой полосы. Действительно,

$$S(i\omega) = \int_{-\infty}^{\infty} \frac{\sin 2\pi F(t - k\Delta t)}{2\pi F(t - k\Delta t)} e^{i n \omega_0 t} dt = \begin{cases} \frac{1}{2F} e^{i k\Delta t \omega} & \text{при } |\omega| < 2\pi F, \\ 0 & \text{при } |\omega| > 2\pi F. \end{cases}$$

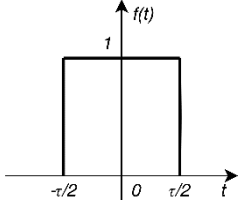
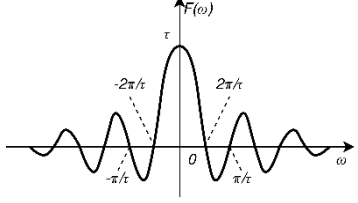
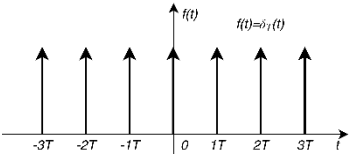
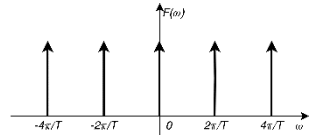
Модуль спектра $S(\omega) = \frac{1}{2F}$. Энергия сигнала через отсчетные значения выражается следующим образом:

$$E = \int_{-\infty}^{\infty} f^2(t) dt = \frac{1}{2F} \sum_{k=-\infty}^{\infty} f^2(k\Delta t). \quad (7)$$

Если полоса частот сигнала $f(t)$ расширяется (таблица 1, п. 1), то Δt будет уменьшаться, и в пределе $F \rightarrow \infty$ функция отсчетов стремится к дельта-функции $t_{\text{н}}(t - t_k)$ (таблица 1, п. 2), а ряд Котельникова (1) превращается в интеграл:

$$f(t) = \int_{-\infty}^{\infty} f(t) t_{\text{н}}(t - t_k) dt. \quad (8)$$

Таблица 1. – Некоторые сигналы и их преобразования Фурье

<p>1. Строблирующая функция</p> $f(t) = G_\tau(t) = \begin{cases} 1 & \text{при } t < \frac{\tau}{2}, \\ 0 & \text{при } t > \frac{\tau}{2}. \end{cases}$		$F(\omega) = \tau \text{Sa}\left(\frac{\omega\tau}{2}\right)$	
<p>2. Немодулированная периодическая последовательность дельта-функций</p> $f(t) = \delta_T(t) = \sum_{n=-\infty}^{\infty} \delta(t - nT)$		$F(\omega) = \omega_0 \delta_{\omega_0}(\omega) = \omega_0 \sum_{k=-\infty}^{\infty} \delta(\omega - k\omega_0)$ $\omega_0 = 2\pi/T$	

Свертка дельта-функции с любой функцией $f(t)$ дает равенство:

$$\int_{-\infty}^{\infty} f(t) t_{\text{и}}(t - t_k) dt = f(t_k) \int_{-\infty}^{\infty} t_{\text{и}}(t - t_k) dt = f(t_k),$$

из которого видно, что интеграл (8) не изменится от замены функции $f(t)$ ее значением $f(t_k)$. Следовательно, (8) преобразовывается в интеграл Дюмеля:

$$f(t) = \int_0^t f(\tau) t_{\text{и}}(t - \tau) d\tau. \tag{9}$$

Вернемся к выражению ряда Котельникова (1). Каждое слагаемое этого разложения по физическому смыслу представляет отклик идеального фильтра нижних частот с частотой среза F на весьма короткий импульс, приходящий в момент $t = k\Delta t$ и имеющий площадь, равную мгновенному значению функции $f(t)$ в тот же момент. Отсюда следует, что при передаче сигнала $f(t)$ с ограниченным спектром по каналу связи необходимо через равные интервалы $\Delta t = \frac{1}{2F}$ взять отсчеты мгновенных значений сигнала и передать по каналу короткие импульсы, площади которых пропорциональны этим отсчетам. На приемном конце эти импульсы пропускаются через фильтр нижних частот, а исходный сигнал $f(t)$ восстанавливается как сумма откликов фильтра. Сигнал длительности T будет определяться $\nu = \frac{T}{\Delta t} = 2TF$ отсчетами.

$$G_\tau(\omega) = \frac{\tau_{\text{и}}}{T} \sum_{k=-\infty}^{\infty} \frac{\sin(k\Omega\tau_{\text{и}}/2)}{k\Omega\tau_{\text{и}}/2} G_\tau(\omega - k\Omega). \tag{10}$$

Для сигналов с конечной длительностью можно сформулировать теорему отсчетов в частотной области, аналогичную теореме отсчетов во временной области, т.е. теореме Котельникова. Такая возможность следует из симметрии преобразований Фурье относительно переменных ω и t .

Заменяя выражение (1) t на ω , ширину спектра $2\omega_m$ на длительность сигнала T_c , интервал дискретизации $T = \frac{1}{2}f_m$ на $\Omega = \frac{2\pi}{T_c}$, функцию $s(t)$ на $G(\omega)$, получим теорему отсчетов в частотной области:

$$G(\omega) = \sum_{k=-\frac{N-1}{2}}^{\frac{N-1}{2}} G(k\Omega) \frac{\sin \frac{T_c}{2}(\omega - k\Omega)}{\frac{T_c}{2}(\omega - k\Omega)}.$$

Здесь N – число выборок (спектральных линий) функции $G(\omega)$. Суммирование происходит по значениям k от $-(\frac{N-1}{2})$ до $(\frac{N-1}{2})$, включая $k = 0$. Таким образом, спектр сигнала конечной длительности T_c полностью определяется выборками, взятыми с интервалом $\Omega = \frac{2\pi}{T_c}$.

При дискретизации сигнала в частотной области общее число спектральных линий при ширине спектра $2\omega_m$ равно:

$$\frac{2\omega_m}{\Omega} = 2T_c f_m.$$

Заключение

Величины $f(kt)$ функции $f(t)$, сдвинутые на время $T = \frac{\pi}{\omega_m} = \frac{1}{2f_m}$, формируют канал утечки информации в виде амплитудно-импульсно-модулированных сигналов.

Число выборок от $(N - 1)$ до $(N + 1)$. Суммированное число выборок $G(k\Omega)$ спектральных линий по значениям k от $-(\frac{N-1}{2})$ до $(\frac{N-1}{2})$, включая $k = 0$, взятое с интервалами $\Omega = \frac{2\pi}{T_c}$, формирует канал утечки информации в виде амплитудно-импульсных моделированных сигналов.

Список литературы

1. Способ оценки защищенности преобразованного в цифровую форму речевого сигнала в каналах утечки информации / В.К. Железняк, С.В. Лавров, А.Г. Филиппович и др. // Комплексная защита информации: материалы XXIV науч.-практ. конф. / г. Витебск (21–23 мая 2019 г.). – С. 53–59.
2. Анализ ошибки равномерного квантования периодической импульсной последовательностью треугольной формы в спектральной области / В.К. Железняк, К.Я. Раханов, С.В. Лавров и др. // Проблемы инфокоммуникаций. – 2022. – № 1 (15). – С. 39–45.
3. Передача информации в системах подвижной связи / В.Ю. Бабков, М.А. Вознюк, В.А. Петраков и др. – СПб.: СПбГУТ, 1999. – 152 с.

4. Лавров С.В., Железняк В.К., Рябенко Д.С. Оценка защищенности каналов утечки высокоскоростной передачи речевых сигналов в цифровой форме / Комплексная защита информации: материалы XXIV науч.-практ. конф. / г. Витебск (21–23 мая 2019 г.). – С. 74–77.

5. Радиотехнические цепи и сигналы: учеб. пособие для вузов / Д.В. Васильев, М.Р. Витоль, Ю.Н. Горшенков и др.; под ред. К.А. Самойло. – М.: Радио и связь, 1982. – 528 с.

РЕЗОЛЮЦИЯ XXVIII НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ «КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ»

С 23 по 25 мая 2023 года состоялось ежегодное мероприятие Союзного государства – XXVIII научно-практическая конференция «Комплексная защита информации» (далее – Конференция).

Организаторами Конференции выступили:
Постоянный Комитет Союзного государства;
Парламентское Собрание Союза Беларуси и России;
Аппарат Совета Безопасности Российской Федерации.

Конференция прошла при организационной поддержке государственного предприятия «НИИ ТЗИ» (Беларусь) и Медиа Группы «Авангард» (Россия) на базе Белорусского государственного университета транспорта (г. Гомель).

В работе конференции приняли участие 130 представителей Беларуси и России. Среди участников конференции 1 академик, 11 докторов наук, 19 кандидатов наук, среди них 11 профессоров, более десяти доцентов и старших научных сотрудников, 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 Союзного государства.

Особое внимание было уделено рассмотрению следующих вопросов:

- информационная безопасность Союзного государства;
- информационная безопасность объектов критической информационной инфраструктуры;
- противодействие киберпреступности;
- криптография и информационная безопасность;
- нормативно-правовое и кадровое обеспечение информационной безопасности.

Особое место на конференции было отведено обмену опытом по вопросам использования защищенных информационных технологий в различных сферах жизнедеятельности государств-участников Союзного государства в целом и общества на всех этапах развития интеграционных процессов Беларуси и России. Кроме того, участниками конференции отмечена особая роль импортозамещения в сфере информационных технологий как основы обеспечения защиты информации в условиях гибридных угроз коллективной информационной безопасности.

Между участниками конференции состоялся плодотворный обмен мнениями и опытом в области исследований, разработок и внедрения в практику деятельности теоретических, методологических, нормативно-правовых и организационно-технических вопросов обеспечения информационной безопасности.

В ходе работы конференции отмечено значение и актуальность для государств – участников Договора о создании Союзного государства следующих задач и направлений деятельности:

выработка совместных подходов к обеспечению безопасности государственных информационных ресурсов Союзного государства в условиях современных вызовов и угроз на основе Концепции информационной безопасности Союзного государства;

консолидация усилий в части разработки программы Союзного государства, направленной на совершенствование системы защиты информационных ресурсов Союзного государства и государств – участников Договора о создании Союзного государства на период 2024–2028 гг.;

формирование государственного кадрового заказа на специалистов по информационной безопасности, расширение контингента и набора специальностей при подготовке кадров в области информационной безопасности, включая кибербезопасность;

обеспечение условий импортонезависимости от зарубежных технологий путем создания полного цикла разработки и внедрения отечественного программного обеспечения, программных и программно-аппаратных средств защиты информации.

Участники конференции постановили:

1. Одобрить работу оргкомитета и результаты XXVIII научно-практической конференции «Комплексная защита информации».

2. Консолидировать усилия в части реализации положений Концепции информационной безопасности Союзного государства.

3. Провести XXIX научно-практическую конференцию «Комплексная защита информации» в 2024 году в Российской Федерации. Просить Постоянный Комитет Союзного государства сформировать рабочую группу для подготовки и осуществления организационных мероприятий.

4. Проинформировать Постоянный Комитет Союзного государства, Парламентское Собрание Союза Беларуси и России, аппарат Совета Безопасности Российской Федерации об итогах XXVIII научно-практической конференции «Комплексная защита информации».

5. Организовать публикацию материалов Конференции в третьем квартале 2023 г.

Резолюция принята на пленарном заседании Конференции 25 мая 2023 г.

СОДЕРЖАНИЕ

Оргкомитет конференции.....	3
Программный комитет.....	4
Выступление Председателя комиссии Парламентского собрания Союза Беларуси и России по безопасности и обороне Белоконева Олега Александровича.....	5
Участникам научно-практической конференции «Комплексная защита информации».....	7
Приветственное слово начальника Оперативно-аналитического центра при Президенте Республики Беларусь.....	8
Приветствие от Федеральной службы по техническому и экспортному контролю (заместитель начальника управления ФСТЭК России С.В. Бондаренко).....	10
Приветствие Председателя Президиума Национальной академии наук Беларуси академика Гусакова Владимира Григорьевича.....	12
Приветствие участникам конференции от Председателя государственного пограничного комитета Республики Беларусь А.П. Лаппо.....	13

ПЛЕНАРНОЕ ЗАСЕДАНИЕ АКТУАЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОЮЗНОМ ГОСУДАРСТВЕ

Ю.К. Язов, С.В. Соловьев. Методологические аспекты формирования требований к эффективности защиты информации в информационных системах.....	14
А.В. Белевич, С.В. Наливайко, С.Н. Сирисько. Импортозамещение в сфере информационных технологий – комплексный подход к защите информации.....	22
Ю.С. Харин, И.Б. Бережной. Актуальные проблемы криптологии.....	25
Д.Н. Арестович, И.К. Ляшко. Результаты реализации программы Союзного государства в области укрепления информационной безопасности.....	31
К.А. Бочков, Д.В. Комнатный, И.О. Жигалин. Электромагнитный терроризм как новый вид угроз функциональной и информационной безопасности критически важных объектов информационной инфраструктуры.....	33

ЗАСЕДАНИЕ № 1 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

А.А. Хорев. Оценка возможностей перехвата побочных электромагнитных излучений средств вычислительной техники, использующих цифровые интерфейсы.....	39
В.К. Железняк, А.Г. Филиппович, К.Я. Раханов, М.М. Барановский. Принципы обработки данных оценки защищенности каналов утечки речевой информации.....	45
В.В. Гришачев, А.Д. Заболотская. Модель угроз критической информационной инфраструктуры на волоконно-оптических технологиях.....	51
В.А. Дмитриев, С.Н. Касанин, Е.П. Максимович. Защищенность информации, циркулирующей в ВОЛС.....	63
Д.В. Комнатный. Методы расчета помехового электромагнитного поля, проникающего через круглое отверстие в плоском экране.....	66
О.Р. Лукманова. Исследование средств защиты телефонного аппарата от утечки по акустоэлектрическим каналам на виртуальных лабораторных стендах.....	69
М.М. Барановский, А.Г. Филиппович, В.К. Железняк, С.В. Лавров. Обоснование измерительного сигнала для оценки защищенности речевой информации при дискретно-квантованном преобразовании.....	74

В.В. Гришачев, А.Д. Заболотская. Волоконно-оптические закладки в модели угроз речевой информации.....	78
Е.Р. Адамовский, В.К. Железняк, К.Я. Раханов. Метод имитационного моделирования показателей шума квантования аналого-цифрового преобразования.....	83
М.А. Буневич, А.И. Майоров, Т.В. Борботько, И.А. Врублевский. Пленочные оптические экраны для защиты конфиденциальной визуальной информации.....	88

ЗАСЕДАНИЕ № 2

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СОЮЗНОГО ГОСУДАРСТВА БЕЛАРУСИ И РОССИИ

И.И. Лившиц. Оценка доступности системы ЭДО, реализованной на базе собственной ИТ-инфраструктуры.....	91
С.П. Ларин, А.Н. Насевич. Основные механизмы формирования и использования эффекта «виртуальной толпы» при решении задач информационного противоборства....	97
А.Н. Королев, Г.В. Коровин. Планирование целевого применения больших кластеров малых космических аппаратов в условиях деструктивных воздействий.....	102
В.А. Воеводин. О методологической проблеме, препятствующей внедрению страхования информационных рисков в процессы управления информационной безопасностью.....	107
М.А. Тарелкин, А.А. Теплинских. Приоритизация сведений об уязвимостях, атаках, эксплойтах, используемых для прогнозирования угроз безопасности информации, на основе публикаций в сети Интернет.....	111
М. Красницкий. Построение отраслевых и корпоративных центров управления информационной безопасностью.....	117
Е.А. Рафальская, С.П. Ларин. Механизмы мобилизации больших социальных групп при проведении психологических операций в зоне интересов.....	118
А.В. Федорцов. Информационная и кибербезопасность инфраструктур Союзного государства как ключевой фактор обеспечения региональной безопасности.....	121
А.Е. Каретников, А.В. Чуваев. Разработка метода выявления информационного влияния в социальных сетях.....	129

ЗАСЕДАНИЕ № 3

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ

М.Н. Бобов. Философия безопасности киберпространства.....	133
Д.Н. Лахтиков. Особенности предупреждения киберпреступлений.....	141
А.Н. Тукало. Оперативно-розыскное противодействие преступлениям, связанным с протестной активностью граждан (на примере использования возможностей глобальной компьютерной сети Интернет).....	145

ЗАСЕДАНИЕ № 4

КРИПТОГРАФИЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

В.Ю. Палуха, Ю.С. Харин. О применении программного комплекса «ЭАДП» для статистического тестирования выходных последовательностей криптографических генераторов.....	148
С.П. Панасенко. О применимости блокчейн-технологий для хранения и обработки идентификационных данных.....	154
П.О. Бегунец. Искусственный интеллект в системе обеспечения кибербезопасности. Подходы к регулированию.....	159
М.Л. Радюкевич. Метод формирования общего секрета с помощью искусственных нейронных сетей.....	161

И.Н. Маслак, А.Ю. Кулаженко. Искусственный интеллект как помощник специалисту информационной безопасности в области информационной безопасности.....	165
М.А. Казловский. Защита от принуждения в системах электронного голосования.....	168

ЗАСЕДАНИЕ № 5

НОРМАТИВНО-ПРАВОВОЕ И КАДРОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Т.В. Борботько. Система подготовки кадров по специальности «Информационная безопасность».....	172
А.В. Марченко. Актуальные вопросы подготовки кадров в области информационной безопасности.....	174
К.А. Бочков, С.Н. Харлап. Методы обеспечения информационной безопасности при передаче информации в микроэлектронных системах железнодорожной автоматики и телемеханики.....	179
Е.Л. Генгринович. Применение интерактивных сред моделирования в целях повышения киберустойчивости отраслевых критических информационных инфраструктур.....	185
И.Р. Шеховцова. Методы и модели эффективности безопасной системы электронного документооборота.....	191
Е.О. Соколов. Практика независимого аудита бизнес-процессов компании на базе ЭДО.....	194
Т.В. Радыно. Защита персональных данных несовершеннолетних в условиях информационной войны.....	198

ЗАОЧНЫЕ ДОКЛАДЫ

О.К. Барановский. О подходе к оценке степени защищенности объектов информационной инфраструктуры от кибератак.....	202
О.К. Барановский, В.К. Рейшель. Информационно-аналитическое обеспечение деятельности центров кибербезопасности.....	205
О.В. Бойсрав, Н.В. Богущ, М.В. Павленок, Е.С. Белоусова. Поглотители электромагнитного излучения на основе фольгированных материалов для защиты средств обработки информации от воздействия помех.....	209
А.В. Бурделев. Восстановление аналитического задания пороговой k-значной функции в узле защиты информации при неполных данных.....	212
С.С. Врублевский, А.А. Бысов. Определение оптимального маршрута для прокладки VPN-туннелей по комплексной метрике в сети электросвязи специального назначения.....	217
В. Диченкова. Применение методов оптимизации на разных стадиях создания систем защиты информации.....	221
О.А. Копырулина. Научно-техническая проблема категорирования объектов критической информационной инфраструктуры.....	227
О. А. Копырулина. Порядок категорирования объектов критической информационной инфраструктуры на примере ТЭК.....	231
О.А. Копырулина. Проблемы при формировании моделей процесса категорирования объектов критической информационной инфраструктуры.....	234
В.П. Кочин, А.В. Шанцов. Алгоритмы разработки системы защиты информации облачных ресурсов.....	237
М.А. Наумов. Защита данных в эпоху квантовых компьютеров: важность перехода на постквантовую криптографию.....	241
Е.П. Рябова, М.А. Казловский. Криптографические механизмы обеспечения анонимности в системах электронного голосования.....	243
М.В. Мальцев, Ю.С. Харин. О тестировании выходных последовательностей криптографических генераторов на основе частотных статистик.....	248

С.В. Харченко, Д.Ю. Галицкий, В.К. Железняк. Некоторые проблемы поиска пэмин при оценке защищенности видеоинформации персональных компьютеров.....	252
В.А. Герасимов, М.А. Казловский, О.В. Бойправ. Механизмы защиты информации при выработке облачной электронной цифровой подписи.....	256
Е.С. Белоусова, О.В. Бойправ, Д.В. Бордиловская, С.В. Саванович. Поглотители электромагнитного излучения с геометрическими неоднородностями полусферической формы.....	261
В.К. Железняк, С.В. Лавров, А.Г. Филиппович, М.М. Барановский. Формирование каналов утечки речевых сигналов при отсчетно-дискретном преобразовании.....	265
Резолюция XXVIII научно-практической конференции «Комплексная защита информации».....	271

Научное издание

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXVIII научно-практической конференции

Гомель, 25–27 мая 2023 г.

Подписано в печать 01.08.2023.

Формат 60×84 1/8.

Бумага офсетная. Цифровая печать.

Усл. печ. л. 32,2. Уч.-изд. л. 31,1.

Тираж 60 шт. Заказ 064-2023.

Издатель и полиграфическое исполнение:
государственное учреждение образования
«Университет гражданской защиты
Министерства по чрезвычайным ситуациям
Республики Беларусь».

Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий
№ 1/259 от 14.10.2016.

220118, г. Минск, ул. Машиностроителей, 25.



23-25 мая 2023 года