КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXVII научно-практической конференции

КЗИ 2022

24–26 мая 2022 года, Российская Федерация

Постоянный Комитет
Союзного государства Беларуси и России
Аппарат Совета Безопасности РФ
Парламентское Собрание Союза Беларуси и России

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXVII научно-практической конференции
(Российская Федерация, 24–26 мая 2022 года)

Москва
2022

УДК 004(470+476)(061.3)
ББК 32.81
К63

К63 **Комплексная защита информации**: материалы XXVII научно-практической конференции, 24–26 мая 2022 г., — Москва, Медиа Группа «Авангард», 2022 год — 276 с.

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

Адресуется исследователям, практическим работникам и широкому кругу читателей.

УДК 004(470+476)(061.3)
ББК 32.81

ОРГКОМИТЕТ

Сопредседатели:
БЕЛОКОНЕВ Олег Алексеевич, Председатель Постоянной комиссии Палаты представителей по национальной безопасности, председатель Комиссии Парламентского Собрания Союза Беларуси и России по безопасности, обороне и борьбе с преступностью
ХРАМОВ Олег Владимирович, Заместитель секретаря Совета безопасности Российской Федерации

ПРОГРАММНЫЙ КОМИТЕТ

Руководители:
КОВАЛЕНКО Андрей Петрович, доктор технических наук, профессор, член-корреспондент Академии криптографии Российской Федерации
КОНЯВСКИЙ Валерий Аркадьевич, заведующий кафедрой «Защита информации» МФТИ (ФизТех), доктор технических наук, академик РАЕН и академик АЭН Российской Федерации
ХАРИН Юрий Семенович, директор Научно-исследовательского института прикладных проблем математики и информатики БГУ, доктор физико-математических наук, академик НАН Беларуси

СЕКРЕТАРИ

ЗУБКОВ Артем Николаевич, директор НКО «Фонд содействия развитию безопасных информационных технологий»
ЛЯШКО Игорь Константинович, начальник сектора научно-производственного республиканского унитарного предприятие «Научно-исследовательский институт технической защиты информации»

ЧЛЕНЫ ПРОГРАММНОГО КОМИТЕТА:

АВЕТИСЯН Арутюн Ишханович, Академик РАН, доктор физико-математических наук, профессор РАН (РФ)
БОРБОТЬКО Тимофей Валентинович, Заведующий кафедрой «Защита информации» учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», доктор технических наук, профессор (РБ)
КУЧИНСКИЙ Пётр Васильевич, Директор научно-исследовательского учреждения «Институт прикладных физических проблем имени А.Н. Севченко» Белорусского государственного университета, доктор физико-математических наук (РБ)
МЕЛЬНИКОВ Сергей Юрьевич, ФГАОУ ВО «Российский университет дружбы народов», доктор физико-математических наук (РФ)

МЕЩЕРЯКОВ Роман Валерьевич, Институт проблем управления РАН, доктор технических наук, профессор (РФ)

МАЛЬЦЕВ Михаил Владимирович, Заместитель директора по научной работе учреждения Белорусского государственного университета «Научно-исследовательский институт прикладных проблем математики и информатики», кандидат физико-математических наук, доцент (РБ)

ЖЕЛЕЗНЯК Владимир Кириллович, Профессор в учреждении образования Полоцкий государственный университет, доктор технических наук, профессор (РБ)

ЯЗОВ Юрий Константинович, ГНИИИ ПТЗИ ФСТЭК России, Главный научный сотрудник, доктор технических наук, профессор (РФ)

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

№

На № 6/н от 25.05.2022

Участникам
научно-практической конференции
«Комплексная защита информации»

Уважаемые участники конференции!

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

Проведение этого мероприятия, по праву, мы называем значимым и важным событием для профильных специалистов и ученых в области обеспечения информационной безопасности государств-участников Договора о создании Союзного государства, на котором осуществляется обмен мнениями и выработка предложений по решению организационных, правовых и технических вопросов обеспечения защиты информации.

Важное значение нынешнего мероприятия обусловлено не только стремительным техническим прогрессом, но и возникновением новых постоянно трансформирующихся рисков, вызовов и угроз для России и Беларуси в информационной сфере. В этих условиях наши усилия должны быть направлены на обеспечение устойчивости информационной инфраструктуры Союзного государства.

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

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

Приветствие председателя Комиссии Парламентского Собрания по безопасности, обороне и борьбе с преступностью О.А. Белоконева

Уважаемые организаторы,участники и гости конференции!

От имени депутатов Парламентского Собрания и от себя лично приветствую вас на открытии двадцать седьмой научно-практической конференции «Комплексная защита информации».

Это значимое ежегодное событие для специалистов и ученых в области обеспечения информационной безопасности. Важное значение нынешнего мероприятия обусловлено не только стремительным техническим прогрессом, но и возникновением новых постоянно трансформирующихся рисков, вызовов и угроз в информационной сфере. С точки зрения информационного пространства понятия «граница» и «территория государства» носят размытый характер, так как они становятся легко проницаемыми при использовании современных информационных технологий. В условиях беспрецедентных санкций, специальной военной операции в Украине, активной информационной войны, развязанной странами входящими и собирающимися войти в блок НАТО, особо актуальным становится предотвращение использования информационных технологий для решения задач, противоречащих интересам обеспечения мира и стабильности, суверенитета, безопасности государства и его граждан.

В условиях тотальной цифровизации спектр угроз постоянно расширяется. Масштаб и последствия деструктивной деятельности в информационном пространстве неуклонно растут. Особую озабоченность вызывают угрозы, связанные с проведением компьютерных атак на критическую информационную инфраструктуру, на ресурсы органов государственной власти. Всем очевидно, что противодействовать угрозам в информационной сфере в одиночку не в состоянии ни одна мировая держава. Поэтому выстраивание партнерских отношений в правовом поле и развитие сотрудничества в рассматриваемой области – объективная необходимость. Еще одно стратегическое направление – формирование механизмов обеспечения безопасного и стабильного функционирования и развития сети интернет на основе равноправного участия всех членов мирового сообщества. Нам необходимо принять все меры для предотвращения использования информационно-коммуникационных технологий в военно-политических целях, противоречащих международному праву, и осуществления враждебных действий и актов агрессии, для недопущения использования этих технологий в террористических и иных преступных целях, а также для подрыва суверенитета государств и вмешательства в их внутренние дела. 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 начата разработка Концепции информационной безопасности Союзного государства, в конце апреля проведено заседание семинара на тему «Состояние и основные направления развития информационной безопасности Союзного государства в условиях современных вызовов и угроз».

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!

Приветствие заместителя Секретаря Совета Безопасности РФ О.В.Храмова

Добрый день, уважаемые коллеги!

Применение информационно-коммуникационных технологий практически во всех сферах жизнедеятельности сопровождается и возникновением новых угроз информационной безопасности.

Вот уже более четверти века на этой площадке обсуждаются вопросы комплексной защиты информации в Союзном Государстве.

Осуществляется обмен мнениями ведущих специалистов и ученых Беларуси и России в области обеспечения информационной безопасности.

Накопленный за это время уникальный опыт сотрудничества российских и белорусских специалистов и ученых нашел свое воплощение в реализации ряда совместных программ и мероприятий в области информационной безопасности. Сегодня мы находимся в непростых условиях, когда недружественными странами прилагаются неимоверные усилия для замедления интеграционных процессов, происходящих в Союзном государстве.

Поэтому **активизация сотрудничества России и Беларуси** на направлении обеспечения информационной безопасности становится **жизненно необходимой** и создает **дополнительные скрепы** братской дружбы наших стран.

По инициативе **Парламентского Собрания Союза Беларуси и России** аппаратами Советов Безопасности Российской Федерации и Республики Беларусь во взаимодействии с профильными органами наших государств разработан **проект Концепции информационной безопасности Союзного государства**.

Основу проекта документа составляют ключевые положения национальных нормативных правовых актов в сфере обеспечения информационной безопасности – **Концепции информационной безопасности Республики Беларусь** *(от 18 марта 2019 г.)* и **Доктрины информационной безопасности Российской Федерации** *(от 5 декабря 2016 г.)*.

Дух и буква этих документов стратегического планирования наглядно демонстрируют **существенную близость** наших подходов к парированию угроз в информационной сфере.

Проект Концепции представляет собой систему официальных взглядов на **цель**, **задачи** и **механизмы** обеспечения информационной безопасности Союзного государства и является основой для формирования **единой государственной политики** в этой области.

Констатируется, что **информационная безопасность Союзного государства** представляет собой **состояние защищенности личности, общества и государства от внутренних и внешних угроз в информационной сфере.**

Сформулированы **общие принципы** информационной безопасности Союзного государства, к которым относятся **мирное урегулирование** споров и конфликтов, **неприменение силы**, **невмешательство во внутренние дела** иных государств, **уважение прав и свобод** человека.

В целях выработки **единой методологии** для реализации государственной политики в этой области в документе приводятся определения понятий «**информационная сфера**», «**угрозы безопасности в информационной сфере**», «**обеспечение информационной безопасности**» и «**силы обеспечения информационной безопасности**».

Стратегическим целеполаганием документа является защита национальных интересов Беларуси и России в информационной сфере путем формирования и устойчивого развития **единого безопасного информационного пространства Союзного государства**.

Для достижения этой цели нам вместе на системной основе необходимо обеспечить решение **задач** по следующим **направлениям**:

- повышение защищенности информационной инфраструктуры государств – участников и недопущение иностранного контроля за ее функционированием;
- формирование единой безопасной среды оборота достоверной информации;
- создание системы совместного прогнозирования, предупреждения и ликвидации последствий от реализации угроз информационной безопасности Союзного государства;
- повышение эффективности противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий;
- обеспечение защиты информации, доступ к которой ограничен национальными законодательствами государств – участников;
- обеспечение технологической независимости путем развития совместного научного и производственного потенциала Союзного государства;
- содействие формированию системы международной информационной безопасности.

Основными **нормативными механизмами** решения указанных задач являются:

- **программы Союзного государства и государственные программы** в области обеспечения национальной безопасности государств – участников;
- **межгосударственные программы взаимодействия** государств – участников по вопросам совместного обеспечения информационной безопасности;
- **целевые и отраслевые программы и планы** государственных органов и организаций, осуществляющих деятельность на территории государств – участников.

Организация взаимодействия органов Союзного государства с государственными органами и организациями государств – участников будет осуществляться по линии **рабочих органов советов безопасности Российской Федерации и Республики Беларусь**.

В практическом плане важно, что разрабатываемая Концепция нацелена **на выработку конкретных мер** совершенствования национальных систем обеспечения информационной безопасности государств – участников в интересах повышения защищенности **общего информационного пространства**.

Уважаемые коллеги! В апреле текущего года в Минске под эгидой аппаратов советов безопасности Российской Федерации и Республики Беларусь прошли **двусторонние межведомственные консультации** по рассмотрению **проекта Концепции информационной безопасности Союзного государства**.

По итогам консультаций подписан протокол**,** в соответствии с которым дальнейшая организационная работа по подготовке к утверждению документа **Высшим Государственным Советом Союзного государства** будет осуществляться по линии **национальных Министерств иностранных дел** с представлением проекта в **Постоянный Комитет Союзного государства**.

Уверен, что предметное обсуждение различных аспектов обеспечения информационной безопасности Союзного государства в кругу высокопрофессиональных и авторитетных участников конференции внесет значимый вклад в решение поставленных задач.

Уважаемые участники конференции! В условиях масштабной цифровизации особую актуальность приобретают вопросы применения **технологий искусственного интеллекта.**

Обсуждению проблематики прикладного применения технологий искусственного интеллекта в военной области, в сфере внутренней безопасности и гражданском секторе экономики посвящена работа профильной секции.

Всестороннее рассмотрение вопросов **криптографической и технической защиты информации**, а также повышения эффективности **кадрового обеспечения** в области информационной безопасности также состоится в рамках **специальных секций конференции**.

Желаю Вам плодотворного сотрудничества и новых профессиональных успехов!

Приветствие начальника Оперативно-аналитического центра при Президенте Республики Беларусь А.Ю.Павлюченко

Уважаемые организаторы и участники конференции!

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

Сегодня применение современных информационно-коммуникационных технологий способствует укреплению экономики за счет предоставления конкурентных преимуществ организациям, обеспечивая эффективность производства и рост производительности труда.

В условиях беспрецедентного санкционного давления развитие системы защиты информационных ресурсов Союзного государства является одним из ключевых направлений обеспечения национальных интересов в области цифровой экономики.

В настоящее время правительствами и иными государственными органами наших стран принимаются необходимые меры по предотвращению деструктивного информационного воздействия на объекты критической информационной инфраструктуры.

Являясь ежегодно проводимым мероприятием Союзного государства, конференция способствует повышению эффективности указанных мер, представляет возможность обсудить актуальнее проблемы в области защиты информации и позволяет уполномоченным государственным органам определить перспективные направления обеспечения кибербезопасности объектов информационной инфраструктуры Республики Беларусь и Российской Федераири.

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

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

УДК 004.056

РЕЗУЛЬТАТЫ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ УКРЕПЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЮЗНОГО ГОСУДАРСТВА

А.Н. ГОРБАЧ, 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 завершается 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»), утвержденной Постановлением Совета Министров Союзного государства от 11 июня 2018 года № 5.

Целью Программы является 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, являются:

- 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).

Государственным заказчиком Программы от Республики Беларусь выступает Оперативно-аналитический центр при Президенте Республики Беларусь.

Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации» в соответствии с приказом Оперативно-аналитического центра при Президенте Республики Беларусь принимает участие в научно-организационном сопровождении и осуществляет мониторинг реализации Программы.

Для исполнителей от Республики Беларусь предусмотрено выполнение работ по 6 мероприятиям Программы, а именно три НИР и восемь ОКР.

В настоящее время исполнителями от Республики Беларусь завершены одна НИР и пять ОКР в рамках четырех мероприятий Программы, продолжаются работы по выполнению двух НИР и трех ОКР в рамках четырех мероприятий Программы.

НИР «Исследование уязвимостей автоматизированных систем управления на критически важных объектах (АСУ КВО) Республики Беларусь и Российской Федерации, разработка описательных моделей угроз, атак, видов защиты их ресурсов» (шифр «Защита-М»).

ОКР «Разработка специализированных радиопоглощающих покрытий» (шифр «Покрытие»).

ОКР «Создание программно-аппаратного комплекса, позволяющего обнаруживать аномалии в сетевом потоке автоматизированных систем управления на критически важных объектах» (шифр «Мамонт»).

ОКР «Разработка программного комплекса мониторинга событий безопасности информационных систем инфраструктуры открытых ключей» (шифр «Монитор»).

ОКР «Совершенствование инфраструктуры открытых ключей на основе современных WEB-технологий» (шифр «Доступность»).

ОКР «Разработка программно-аппаратного комплекса выявления специальных технических средств негласного получения информации, передающих информаци по сетям сотовой связи (шифр «База»).

ОКР «Разработка программного комплекса обеспечения IP-коммуникаций для мобильных устройств, работающих под управлением операционной системы Android (серверное

и клиентское приложение) с применением шифрования передаваемых данных» (шифр «Болеро»).

НИР «Совершенствование криптографической инфраструктуры Республики Беларусь» (шифр «Криптограф»).

ОКР «Разработка комплексного инструментария поиска в программном обеспечении недекларируемых возможностей (скрытого и/или не описанного функционала, ошибок)» (шифр «Поиск»).

ОКР «Разработка комплекса, реализующего сбор, анализ и корреляцию событий информационной безопасности критической инфраструктуры, с учетом использования защищенного репутационного сервиса» (шифр «Шкала»).

НИР «Разработка предложений по направлениям исследований в области совершенствования системы защиты общих информационных ресурсов Союзного государства на основе анализа результатов выполнения мероприятий программы Союзного государства» (шифр «Источник»).

В качестве исполнителей Программы с белорусской стороны выступают государственное предприятие «НИИ ТЗИ», Республиканское унитарное предприятие «Национальный центр электронных услуг», научно-исследовательское учреждение «Институт прикладных физических проблем им. А.Н. Севченко» Белорусского государственного университета, учреждение Белорусского государственного университета «Научно-исследовательский институт прикладных проблем математики и информатики», закрытое акционерное общество «НТЦ Контакт», общество с ограниченной ответственностью «СЕКЬЮРИТИ ЛАБ». общество с ограниченной ответственностью «СмартФорт».

По результатам анализа проводимых исследований в Республике Беларусь в области защиты общих информационных ресурсов и систем информационно-телекоммуникационной инфраструктуры Союзного государства, хода их выполнения установлено, что все исследования проведены в соответствии с техническими заданиями по заключенным договорам. Сроки выполнения этапов НИОКР совпадают со сроками, указанными в ранее утвержденных планах-графиках выполнения НИОКР. Все работы по мероприятиям Программы, предусмотренные заключенными договорами, исполнителями выполнены полностью в установленные сроки.

Результаты реализации мероприятий Программы соответствуют поставленным цели и задачам.

За счет объединения интеллектуальных и материальных потенциалов Республики Беларусь и Российской Федерации результаты выполнения Программы обеспечат:

- принятие эффективных мер по выявлению, предупреждению и пресечению (снижению эффективности) несанкционированного доступа к информационным ресурсам в информационных системах Союзного государства и государств-участников при их взаимодействии и совместном использовании;
- устойчивое функционирование информационных систем Союзного государства и государств-участников при их взаимодействии и совместном использовании;
- сохранение и развитие научно-технического, технологического и производственного потенциала, повышение конкурентоспособности промышленной продукции;
- предотвращение чрезвычайных ситуаций, связанных с нарушением функционирования автоматизированных систем управления технологическими процессами на критически важных объектах Республики Беларусь и Российской Федерации при их взаимодействии и совместном использовании.

Положительный эффект от реализации мероприятий и Программы в целом оценивается величиной чистой экономии бюджетных средств за счет создания единых для Союзного государства и государств-участников научно-технических условий, необходимых для реализации мер по предупреждению и нейтрализации угроз безопасности информации в информационных системах Союзного государства и государств-участников при их взаимодействии и совместном использовании и, как следствие, исключение дублирования в разработке методов (способов) и средств защиты информации республиканскими органами государственного управления, федеральными органами исполнительной власти и организациями Республики Беларусь и Российской Федерации, если бы они такую разработку осуществляли самостоятельно.

Основными направлениями практического использования результатов реализации Программы являются:

- организация 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.

Список литературы

1. Постановление Совета Министров Союзного государства от 11 июня 2018 г. № 5 О программе 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»)

УДК 007.51

ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ СОЮЗНОГО ГОСУДАРСТВА

Р.Ф. НАРДИНОВ

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

В рамках прошедшей 16 мая 2022 года в г. Москве встречи лидеров государств – членов Организации договора о коллективной безопасности Президентом Республики Беларусь А.Г.Лукашенко отмечено, что в настоящее время против нас развернута гибридная война с составляющей частью, в которой основой является информационная война.

Сегодня деструктивное информационное воздействие на информационную инфраструктуру является одним из инструментов вмешательства во внутренние дела государств – участников Союзного государства.

В период после завершения выборов Президента Республики Беларусь в 2020 году отмечается рост кибератак на объекты информационной инфраструктуры – информационные системы и ресурсы государственных органов и организаций республики, некоторые из них привели к киберинцидентам с достаточно существенными последствиями.

Одной из мер, принимаемых для предотвращения киберинцидентов и минимизации их последствий, является развитие государственных систем обнаружения кибератак и реагирования на инциденты безопасности в информационной инфраструктуре.

В развитие государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) в органах (организациях) предусматривается создание структурных подразделений, осуществляющих функции по обеспечению информационной безопасности, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты [1].

В Республике Беларусь проводятся мероприятия по созданию национальной системы обеспечения кибербезопасности. Основными элементами системы предусматриваются Национальный центр мониторинга кибербезопасности и реагирования на киберинциденты и ведомственные центры мониторинга кибербезопасности и реагирования на киберинциденты.

Одним из ключевых направлений обеспечения защиты информационных ресурсов Союзного государства является взаимодействие Национального координационного центра по компьютерным инцидентам ГосСОПКА и Национального центра мониторинга кибербезопасности и реагирования на киберинциденты Беларуси.

В целях повышения эффективности мероприятий по обеспечению кибербезопасности в Союзном государстве целесообразно установить и внедрить новые формы такого взаимодействия.

В условиях санкционного давления, оказываемого на государства – участников Союзного государства, видится целесообразным принять меры, направленные на импортозамещение средств защиты информации, а также гармонизацию законодательства в целях обеспечения возможности введения в гражданский оборот средств защиты информации отечественного производства на территории Республики Беларусь и Российской Федерации.

С учетом развития информационных отношений между субъектами государств – участников Союзного государства к одному из направлений развития системы защиты информационных ресурсов Союзного государства целесообразно отнести развитие механизмов цифрового доверия в информационных инфраструктурах Беларуси и России.

Гармонизация законодательства об электронной идентификации и услугах доверия при межгосударственном электронном взаимодействии, разработка и реализация механизмов для взаимного признания электронной идентификации пользователей позволят обеспечить развитие системы межгосударственного электронного взаимодействия, в том числе в целях решения задач по обеспечению информационной безопасности.

В настоящее время остро стоит вопрос обеспечения государственных систем обнаружения кибератак и реагирования на инциденты безопасности в информационной инфраструктуре квалифицированным персоналом.

В этой связи подготовка квалифицированных кадров в сфере обеспечения кибербезопасности является одним из приоритетных направлений развития системы защиты информации Союзного государства.

Для решения задачи кадрового обеспечения требуется разработка государственных образовательных стандартов по специальностям высшего образования и направлениям подготовки в области информационной безопасности, формирование учебно-методического обеспечения подготовки кадров, государственного заказа на подготовку кадров в области обеспечения кибербезопасности.

Одним из вариантов решения данной задачи является переподготовка специалистов, имеющих высшее образование по техническим специальностям в области информационно-коммуникационных технологий, в специализированных образовательных центрах (учреждениях).

Развитие системы защиты информации в информационных системах Союзного государства целесообразно считать одним из приоритетных направлений и первоочередных задач дальнейшего развития Союзного государства.

Государственными заказчиками программы Союзного государства «Паритет» проводится работа по формированию проекта концепции новой программы Союзного государства, направленной на научно-техническое обеспечение принимаемых мер по обеспечению безопасности объектов информационной инфраструктуры государств-участников Союзного государства.

К основным направлениям научных исследований и разработок в рамках данной программы следует отнести:

- обеспечение функционирования государственных систем обнаружения кибератак и реагирования на инциденты безопасности в информационной инфраструктуре (разработка, модернизация и сопровождение средств, предназначенных для обнаружения, предупреждения и ликвидации последствий кибератак, использование методов искусственного интеллекта для создания средств оценки эффективности защищенности объектов информационной инфраструктуры от кибератак, прогнозирования ситуации в области обеспечения кибербезопасности);
- разработку нормативных правовых документов (технических нормативных правовых актов, государственных образовательных стандартов и иных документов) в области обеспечения кибербезопасности;
- разработку средств технической и криптографической защиты информации, контроля ее защищенности.

Список литературы

1. Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

УДК 007.51

РОЛЬ БАНКА РОССИИ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ

В.А.УВАРОВ

Департамент информационной безопасности Банка России

Уважаемые коллеги, участники и гости!

Я рад приветствовать всех на Конференции «Комплексная защита информации». Я искренне благодарен организаторам за предоставленную возможность поделиться на этой площадке нашими результатами, оценками и прогнозами.

Прежде всего хотел бы сказать, цифровая трансформация стала неотъемлемой частью нашей жизни. Её внедрение оказало влияние на все сферы: здравоохранение, образование, транспортная инфраструктура и, конечно, финансовая сфера. И очевидно, что с ростом цифровизации стали появляться и новые риски, связанные с киберугрозами. Эти риски, требуют от нас очень оперативного, качественного и своевременного реагирования. Наша главная задача состоит в том, чтобы обеспечить своими мерами действенную защиту, как самих финансовых организаций, так и их клиентов – наших граждан от кибермошенников. Конечно, говоря о 21 годе, нельзя не упомянуть пандемию. Она не только ускорила цифровую трансформацию финансового сектора, но и прочна вошла в цифровую и новостную повестки. И на это не могли не обратить внимания мошенники. Они вообще очень оперативно отслеживают все новости, тренды и изменения и очень умело встраивают эту информацию в свои схемы. Многочисленные заявления о выплатах, компенсациях, цифровых кодах, вакцинациях – это лишь часть того, что они использовали для обмана людей. Сейчас же активизировались мошенники с предложением получить якобы «компенсационную» выплату, если ранее гражданин стал жертвой мошенников. Это так называемый вариант схемы «обман на обмане», жестокость которого заключается в том, что злоумышленники бесчеловечно наживаются на гражданах, которые ранее уже пострадали от рук злоумышленников. В целях оповещения наших граждан о этой и других актуальных мошеннических схемах, мы в мае запустили на сайте Банка России раздел по противодействию мошенническим практикам. В нем в простой и доступной форме публикуем описание популярных и актуальных схем, и советы для наших граждан. Очень важно оперативно предупреждать о актуальных рисках и давать практические советы, ведь у мошенников выстроена системная работа: они как живой организм – приспосабливаются к постоянным изменениям окружающей среды. За их звонками и рассылками, как правило, стоит не один человек, а группы лиц, где четко прописана роль каждого участника, где каждое движение и фраза продуманы до мелочей. Например, тексты для обзвонов и возможные варианты ответов тщательно отрабатываются психологами. Действуют мошенники быстро, агрессивно, не давая жертве одуматься и оценить предпринимаемые действия и шаги.

Перейду к конкретным цифрам. На слайде представлена динамика по основным показателям хищений денежных средств у граждан. В 2021 году мы наблюдали рост по операциям без согласия клиентов, как по объему: в прошлом году было похищено 13,5 млрд. руб. против 9,8 млрд. руб. 2020 года, так и по количеству – на практически 34% возросло число операций без согласия клиентов. В целом, эти изменения происходили на фоне естествен-

ного роста и появления новых финансовых услуг, и объем переводов с помощью электронных средств платежа тоже вырос порядка на 29%. Меньше недели назад на нашем сайте мы опубликовали данные по операциям без согласия клиентов за 1 квартал 2022 года. За первые 3 месяца текущего года в канале терминалов, банкоматов, импринтеров отмечается рост количества и объема хищений. Мы фиксируем, что в этот период злоумышленники активно применяли комбинированные схемы мошенничества, при которых граждан вынуждали совершать перевод через этот канал, что привело к росту в нем показателей операций без согласия клиентов. Например, мошенники в таких схемах вынуждали граждан внести денежные средства на названные ими счета через терминалы.

Если говорить про основные угрозы прошедшего года – то, конечно это мошенничество с использованием социальной инженерии. Несмотря на то, что в числовом значении количество таких операций снизилось с 61% до 49%, тем не менее ущерб от них наиболее значительный, так как каждый раз, когда человек попадает на удочку мошенников, они наносят ему очень сильный ущерб. Бывает так, что граждан не только лишают имеющихся средств, но и оставляют с обязательствами по кредитам. Поэтому это самый опасный вид операции. Основным каналом атак по-прежнему остается телефон, это порядка 80%. Следующим каналом атаки являются интернет ресурсы, на которые наши граждане заходят самостоятельно (это фишинговые сайты, различные рекламные банеры, социальные сети) и соответственно, оставляют там свои персональные данные платежную информацию (10%).

Очевидно из всего вышесказанного, что направление борьбы с кибермошенниками является одним из приоритетных в Банке России. Но, как показывает практика, простых и быстрых решений, т.н. «серебряной пули» здесь нет, необходим комплексный подход на системной основе с привлечением всех заинтересованных сторон (государственных структур, правоохранительных органов, финансовых организаций и операторов связи), создание единого информационного поля и механизма эффективного взаимодействия. Этим мы сейчас активно занимаемся, и надо отметить, находим поддержку у наших коллег и контрагентов.

Если говорить конкретно, то меры по борьбе с любым негативным явлением можно разделить на три основные части: первое – это предупреждение правонарушений, их еще называют профилактическими мерами; второе – выявление действий и схем злоумышленников, третье – пресечение правонарушений с привлечением виновных к ответственности.

По всем этим направлениям Банк России в рамках своей компетенции предпринимает значительные усилия.

С точки зрения соотношения затрат к результатам самыми эффективными являются меры профилактики. Потому что, поскольку они позволяют предотвратить нанесение ущерба гражданам и избежать дальнейших затрат государства по поиску и привлечению к ответственности злоумышленников.

И в первую очередь важной отраслью профилактики является повышение киберграмотности граждан. Для этого разработаны информационно-просветительские материалы по безопасному поведению: это тематические плакаты, видеоролики, листовки. Мы взаимодействуем с ФОИВ и ведомствами, а также представителями власти (например, Минпроторг, Минобр, Минтруд, Минздрав, МВД и многие другие) по размещению нашего контента на объектах транспортной и социальной инфраструктуры. Получили много положительных откликов и подтверждений готовности реализовывать кампании совместно. И сейчас наш контент размещают в МФЦ, поликлиниках, и больницах, домах культуры, библиотеках, учреждениях социальной защиты населения, образовательных учреждения. Цель, которую мы преследуем – сформировать безопасную модель поведения человека и развить базовые навыки кибергигиены.

Активно продвигаем вопросы обучения специалистов в сфере информационной безопасности. Так, за время реализации практико-ориентированной программы обучения «КиберКурс» на базе Университета Банка России бесплатное обучение прошли порядка 9500 специалистов в сфере ИБ, включая более 5000 представителей служб ИБ организаций кредитно-финансовой сферы. Банком России разработан проект профстандарта «Специалист по ИБ в кредитно-финансовой сфере». И, конечно, постоянно работаем по тематике повышения киберграмотности с финансовыми организациями, оказываем практическую и методическую помощь, разрабатываем соответствующие рекомендации, в которых детализированы подходы о том, каким образом банки должны доводить значимую информацию до клиентов.

И последний блок в направлении профилактических мер – разработка и поддержка различных законодательных инициатив.

Нам удалось довести до принятия несколько законов очень важных которые длительное время находились на этапе первого чтения. Закон о блокировки сайтов который предоставил Банку России право совершать блокировку через Генеральную прокуратуру вступил с 1 декабря 2021 года, так же закон о запрете подмены номера, там сейчас готовят подзаконную нормативную базу для действий уже в этом году, так же был законопроект, о регистрации сайтов. Продолжается работа над законопроектом о создании Единой информационной системы проверки сведений об абоненте и пользователях услугами связи. Законопроектом предусмотрено, что мобильные операторы будут предоставлять в систему следующую информацию:

- о статусе абонентского номера,
- о подтверждении сведений об абонентском номере,
- смене пользовательского оборудования абонентом

Мы полагаем, что скорейшее принятие законопроекта будет являться действенной и продуктивной мерой для борьбы с телефонным мошенничеством.

Переходя дальше, если меры профилактики не сработали, включается следующий комплекс мер, по выявлению действия мошенников и противодействию им.

И здесь я хочу напомнить о нашем основном инструменте в части выявления и реагирования на инциденты ИБ – это Финцерт Банка России. Я остановлюсь подробно на количественных результатах.

1. В части борьбы с телефонными мошенниками.

За 2021 год мы направили на блокировку информацию по более чем 179 тыс. телефонных номеров, используемых в мошеннических целях, это выше аналогичного показателя прошлого года в 7 раз. Только за 1 квартал 2022 года размер этого показателя уже составил практически 90 тыс. номеров. В мае мы наблюдаем рост активности телефонного мошенничества. По предварительным данным, с начала месяца мы уже инициировали блокировку более 25 тыс. номеров, что на 13% больше, чем в апреле, и в три раза превышает показатель заблокированных номеров в марте. По нашим данным, с городских номеров мошенники звонят в 3-4 раза чаще, чем с мобильных.

Если говорить о противодействии Интернет-мошенникам, то здесь мы работаем в 2 направлениях: с регистраторами доменных имен и Генеральной прокуратурой. За 2021 год мы направили в адрес регистраторов доменных имен, информацию о более чем 6 тыс. 200 сайтах для последующего снятия их с делегирования. А по второму направлению – совместно с Генеральной прокуратурой – за период нашего взаимодействия с 2020 года по 20 мая текущего года направили на блокировку практически 5 тыс. 800 ресурсов, из них за

2021 год – 3100 сайтов. В 2021 и 1 квартале 2022 года злоумышленники чаще всего маскировали фишинговые сайты под сайты действующих кредитно-финансовых организаций. Кроме того, они активно использовали сайты с информацией о возможности получения компенсационных выплат от государства или о возможности заработать денежные средства за прохождение опроса или теста.

Ключевым фактором в такой работе является скорость реакции, чем быстрее мы блокируем инструменты мошенников, тем меньшее количество людей пострадает от их действий. И мы с коллегами из других ведомств последовательно движемся по повышению оперативности нашего взаимодействия.

Объектами злоумышленников в начале года стали не только клиенты банков. Сами банки ощутили на себе кратное увеличение хакерских атак. По нашим данным их количество увеличилось более чем в 20 раз в феврале 2022 года. Следует отметить, что в целом финансовые институты выдержали нападки и смогли бесперебойно осуществлять платежные операции и предоставлять сервисы. Те не менее, исходя из анализа складывающейся обстановки и выявления новых факторов и угроз, мы планируем развивать и внедрять меры по совершенствованию защиты финансовой системы.

Наш центр взаимодействия и реагирования работает 24/7, и не останавливаясь ни на секунду, продолжает оперативный обмен информацией об угрозах, взаимодействие с широким кругом субъектов, а также реагирование на компьютерные атаки.

В настоящее время АСОИ ФинЦЕРТ – это своего рода «озеро данных» (Data Lake), в котором аккумулируется и обрабатывается большой массив информации о компьютерных атаках и инцидентах информационной безопасности всей кредитно-финансовой сферы. По результатам анализа этой информации ФинЦЕРТ Банка России предоставляет организациям кредитно-финансовой сферы – участникам информационного обмена необходимые сведения для защиты от компьютерных атак, направляя сообщения об уязвимостях в ПО и бюллетени по безопасности со сводкой актуальных угроз.

В части защиты прав и законных интересов наших граждан – Банком России совместно с правоохраной и банками разработан ряд механизмов, цель которых – защитить граждан от действий мошенников. Это наш приоритет и на 2022 год.

В частности, законопроект об информационном обмене Банка России с МВД России по операциям без согласия клиентов. Банк России считает особенно важным поддержать меры, направленные повышение скорости и эффективности расследования уголовных дел по эпизодам указанного типа мошенничества. В настоящее время правоохранительные органы действительно тратят существенное количество времени на получение в кредитных организациях информации о счетах, через которые выводили похищаемые средства.

Реализовать это предлагается путем осуществления оперативного взаимодействия МВД РФ с Банком России посредством нашей технологической инфраструктуры– АСОИ ФинЦЕРТ.

Задачи по обеспечению защиты интересов наших граждан и налаживанию взаимодействия с МВД являются приоритетными и на 2022 год в части законопроектной работы.

Мы рассчитываем, что комплекс законодательных изменений позволит повысить качество работы по борьбе с кибермошенниками и в конечном счете позволит сохранить деньги наших граждан.

Как изменились наши векторы развития с приходом 2022 года?

Кибератаки, это не последнее с чем мы столкнулись в 2022 году. Уход с российского рынка иностранного ПО, техники, ИТ-сервисов и продуктов определил необходимость в

ускоренном импортозамещении для поддержания операционной надежности финансовых организаций на высоком уровне. Сейчас вопросы импортозамещения по кибербезопсаности вышли на приоритетный уровень. В целях формирования комплексного подхода к импортозамещению в соответствии с Указом Президента №166, мы совместно с коллегами из Минцифры, Минпромторга и участниками финансового рынка прорабатываем вопрос создания отраслевых центров компетенции импортозамещения программного обеспечения на базе организаций КФС. Следует отметить, то за нами в рамках полномочий остается вопрос координации по установлению требований по обеспечению операционной надежности во взаимодействии с Минцифры России, Минпромторгом России. В перечень организаций, на базе которых будет проводится тестирование ИТ-решений для импортозамещения в финансовом секторе экономики, включены системообразующие организации с государственным участием, имеющие значимые объекты КИИ.

Резюмируя, отмечу, что мы рассчитываем, что все наши законодательные инициативы и меры принесут реальную пользу гражданам и позволят финансовым организациям сохранить стабильность в области обеспечения операционной надежности в это непростое время.

В рамках реализации этих направлений крайне важно сотрудничество и координация совместных усилий между Банком России, правоохранительными органами, ведомствами и организациями кредитно-финансовой сферы. И только такой, ответственный подход, с максимальной вовлеченностью всех сторон на наш взгляд даст свои плоды в вопросах борьбы с кибермошенничеством и станет действенным способом защиты прав и законных интересов наших граждан!

И в завершении своего выступления хотел бы отметить, что Департамент информационной безопасности всегда открыт к диалогу и готовы к сотрудничеству в целях борьбы с киберпреступностью. Спасибо Вам за внимание!

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — СТРАТЕГИЧЕСКИЙ ПРИОРИТЕТ СОЮЗНОГО ГОСУДАРСТВА

ОСНОВНЫЕ НАПРАВЛЕНИЯ БЕЗОПАСНОСТИ КИБЕРПРОСТРАНСТВА

М.Н. БОБОВ

УО Белорусский государственный университет
информатики и радиоэлектроники
г. Минск, 220119, Беларусь

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[1]. Наиболее приемлемые трактовки этого определения, следующие:

1. Пространство функционирования продуктов информационно-коммуникационных технологий, позволяющих создавать чрезвычайно сложные системы взаимодействий агентов с целью получения, обмена и управления информацией, а также осуществления коммуникаций в условиях множества различных сетей.
2. Сложная сущность, которая реально существует в виде глобальной совокупности процессов взаимодействия людей, программного обеспечения и сервисов Интернет в сетях (включая подключенное к ним технологическое оборудование), но которая при этом никак не проявляется в какой-либо известной, материальной форме.
3. Всеобъемлющая цифровая реальность, являющаяся продуктом информационно-коммуникационных технологий, посредством которой независимо от воли и сознания каждого индивида происходит большинство социальных взаимодействий, создающих новую среду обитания современного человека.

Таким образом, определение киберпространства может быть раскрыто в трех различных аспектах:

1. физический аспект;
2. информационный аспект;
3. социальный аспект.

Наличие определенных устройств (компьютеры, смартфоны, средства виртуальной реальности и т.п.), посредством которых киберпространство создается и функционирует является основным элементом, определяющим его физическую природу.

Информационный аспект киберпространства обуславливает представление киберпространства как совокупности бесчисленных информационных потоков, через которые с невероятной скоростью курсирует информация, переведенная в цифровую форму. Социальный аспект кибернетического пространства связан с рассмотрением всех социальных

взаимодействий, которые происходят в этой неосязаемой цифровой среде, в том числе функционирование многочисленных виртуальных сообществ, а также новые возможности для построения идентичностей.

Определим теперь ключевые характеристики киберпространства как новой среды существования современного индивида [2].

1. Виртуальность.

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.

2.Контроль сети.

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.

3. Неопределённость границ, отсутствие центра.

Третьей характерной чертой киберпространства является его размытость и неопределённость границ. По аналогии с сетью, киберпространство в этом случае характеризуется децентрализацией и не является четко определенным и заданным.

4. Среда для взаимодействия

В-четвёртых, 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.

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 [2]:

- 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.

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 су-

ществование этих технологий является основой стабильного функционирования общества информационной эпохи господства сетевых структур.

В связи с необходимостью обеспечения безопасности киберпространства возникает вопрос, который должен задавать себе каждый, кто погружается в бесконечный, невидимый, непредсказуемый мир киберпространства: «Возможно ли органичное сочетание использования сверхсовременных технологий с традиционным духовными ценностями и идеалами человечества?». Другими словами, 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 в разделе 1?

Ответом на данный вопрос можно считать опубликованный в 2012 году стандарт ISO/IEC 27032 «Наставления по кибербезопасности», разработанный Подкомитетом №27(SC27) по информационной безопасности Первого объединённого технического комитета (JTC1) ISO/IEC [3].

Безопасность и стабильность Киберпространства во многом зависит от безопасности и надежности входящих в него сегментов критической инфраструктуры и тесно связана с безопасностью Интернет, индустриальных, приватных и домашних компьютерных сетей, а также с информационной безопасностью в целом. Другими словами, данный Стандарт представляет собой руководство по повышению уровня безопасности киберпространства в контексте ее уникальности и непересечения с другими доменами безопасности, а именно, такими как:

- информационная безопасность,
- безопасность приватных сетей,
- Интернет-безопасность,
- безопасность ключевых информационных систем объектов критической инфраструктуры.

Позиционирование кибербезопасности на компонентах водящих в него сегментах критических структур, приведено на рис.1

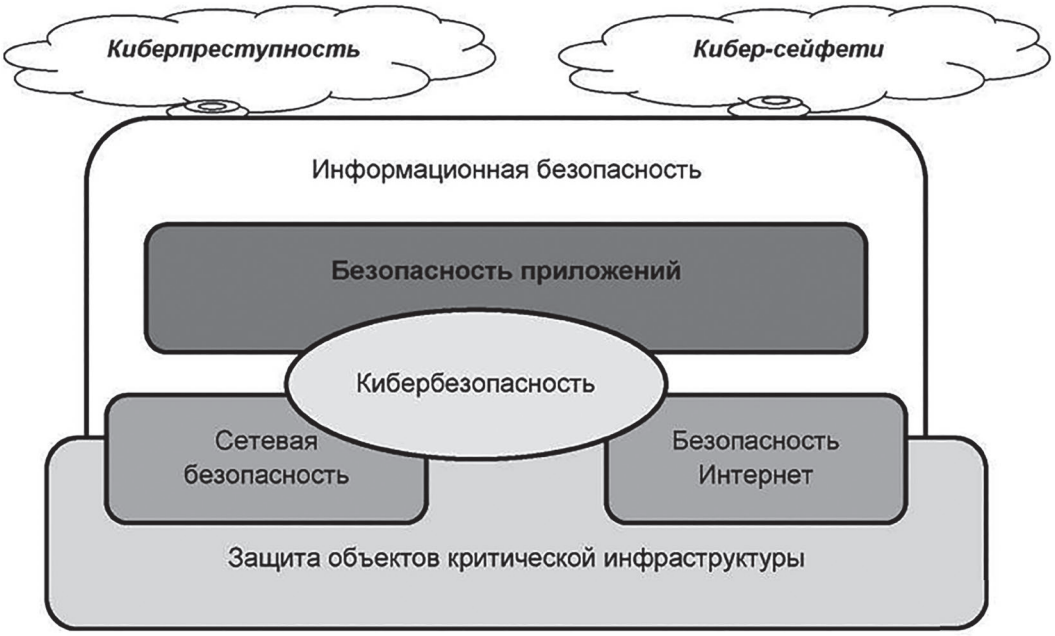


Рисунок 1. Позиционирование кибербезопасности

Первой зоной внимания Стандарта объявляется проблемы, обусловленные разрывами между различными доменами безопасности Киберпространства. 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:
- автономных вредоносных кодов,
- отдельных злоумышленников,
- преступных и агрессивных организаций в Интернет;
- обнаружения и мониторинга атак; и
- 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 участников, в частности, с пониманием того, что разные провайдеры и потребители могут находиться в географически различных регионах, часовых поясах и относиться к различным юрисдикциям.

В стандарте предлагается подход к формированию организационнотехнической системы информационного взаимодействия и обмена информацией, которая включает в себя четыре главные составляющие: 1) политики, 2) методы и процессы, 3) персонал, 4) технику и технологию.

1. Организации, передающие информацию об инцидентах, и организации, принимающие эту информацию должны следовать определённым политикам, содержащим:

- назначение двух типов организаций для формирования передаваемой информации и приёма и обработки получаемой информации;
- категорирование и классификацию различных видов собираемой, обрабатываемой, хранимой и распространяемой информации;
- правила минимизации объёма и содержания распространяемой информации по каждой категории и каждому классу;
- формализацию требований к используемым протоколам, обеспечивающим результативность и эффективность взаимодействия;
- порядок использования ограничений в осведомлении, который при передаче конфиденциальных сведений может сужать круг осведомления в диапазоне от отдельного лица до организации или группы организаций.

2. Для обеспечения надежности и эффективности обмена информацией должны быть реализованы общие правила и процедуры, основанные на соответствующих стандартах используемых в индустриальном секторе для обмена информацией и информационного взаимодействия в контексте кибербезопасности. Правила и процедуры в контексте кибербезопасности должны включать в себя:

- категорирование и классификацию сведений, подлежащих распространению;
- соглашение о конфиденциальности между участниками взаимодействия, входящими в состав организационнотехнической системы информационного обмена;
- разработку планов и графиков обмена информацией и информационного взаимодействия, с учётом специфики различных организаций и подразделений и регламента их работы;
- разработку методик и программ проведения регулярного тестирования уровня безопасности информационного взаимодействия, которая должна выполняться применительно к активам с высокой степенью риска и поддерживаться системой категорирования и классификации данных, принятой в организации;
- использование инструкций, содержащих рекомендации по функциям, ответственностям и обязательствам заинтересованных сторон, которые должны предприниматься соответствующими подразделениями и службами, включенными в процесс обращения с такой информацией.

3. Персонал в организации является ключевым фактором, обеспечивающим достижение и поддерживание заданного уровня кибербезопасности. Категория «персонал» подразумевает индивидуумов, вовлеченных в реализацию методов и процессов информационного взаимодействия и способных влиять на достижение позитивных результатов в отношении кибербезопасности. Поэтому персонал, участвующий в обмене информацией, должен соответствовать определённым требованиям:
   - персонал организации должен быть осведомлен о существовании, появлении или обновлении угроз кибербезопасности путём:
     - регулярного информирования сотрудников о состоянии угроз кибербезопасности, ассоциированных непосредственно с организацией или со сферой ее деятельности;
     - разработки, организации и проведения на регулярной основе семинаров и тренингов, в которых рассматривается и моделируется развитие сценариев кибератак для конкретных ситуаций и сфер деятельности;
     - регулярного тестирования с пошаговым разбором соответствующих сценариев, достижения обучаемыми необходимого уровня понимания материала, знания необходимых сценариев поведения и владения соответствующими инструментальными средствами;
   - персонал должен быть готов к рациональным и результативным действиям, направленным на снижение рисков или реагирование на проявления событий с использованием своих знаний, навыков и опыта;
   - организации, которые запрашивают или предоставляют распространяемую информацию должны вести списки своих контактов и обмениваться этими списками;
   - должны быть составлены отдельные детальные списки контактов в соответствии с политикой ограничения круга осведомления, категорирования и классификации информации;
   - в соответствии с требованием минимизации информации список контактов не должен содержать конфиденциальных персональных данных;
   - списки контактов должны быть защищены от несанкционированного изменения с использованием соответствующих технических средств защиты.
4. В настоящем Стандарте представлены некоторые широко используемые инструментальные средства и технологии унификации данных, которые могут быть рекомендованы для снижения рисков кибербезопасности при информационном взаимодействии и обмене информацией, в том числе:

- единый порядок обращения с информацией, включающий выполнение требований безопасности, защиты и минимизации информации в каждой из ее категорий и в каждом классе, а также предоставление всем причастным сторонам гарантий выполнения этих требований;
- унификация форматов передачи данных, которая обеспечивает упрощение обмена и совершенствование хранения, передачи, использования и совместимости систем информационного взаимодействия между собой (примером такой унификации является набор рекомендаций ITU-T X.1205);
- использование базовых методов и алгоритмов обработки данных, например, таких как вычисление хеш-функций, анонимизаця 1P-адресов и другие виды предварительной обработки;
- отображение информации о событиях путём визуализации данных, что упростит восприятие операторами фактов проявления событий безопасности без вникания в детали;
- использование системы криптографической защиты информации, включая подсистему распределения ключей, для обеспечения возможностей распространения конфиденциальных данных (система должна включать в себя средства резервирования и аварийного восстановления (в том числе ключей);
- обеспечение выполнения требований безопасности, производительности, надежности и эффективности при проведении онлайновых совещаний и оффлайновых дискуссий, обмене текстовыми сообщениями и файлами мультимедиа, используемых участниками организационнотехнической системы информационного обмена для решения задач взаимодействия пользователей.

Список литературы

1. Д.Е. Добринская. Киберпространство: территория современной жизни // Вестник Московского Университета. Сер. 18. Социология и политология. 2018. Т. 24. № 1. С. 52—70.
2. Ю. И. Соколов. Новый вид рисков — риски киберпространства // Проблемы анализа риска. Москва, АО ФИД «Деловой экспресс», Том 13, 2016, № 6. С.6-21.
3. ISO/IEC 27032:2012 — Information technology — Security techniques — Guidelines for cybersecurity.

ВОПРОСЫ ОБЕСПЕЧЕНИЯ КОЛЛЕКТИВНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЮЗНОГО ГОСУДАРСТВА

В.Р. ГРИГОРЬЕВ
Институт кибербезопасности и цифровых технологий, *РТУ МИРЭА,*
г. Москва, *119454,* Российская Федерация

Мы живём в судьбоносное для нашего Союзного государства, да и для всего Мира время. По сути дела, на наших глазах мир переживает переломный этап смены эпох, уход с исторической сцены однополярного порядка по принципу PAX AMERICA и формирование

полицентричного миропорядка. Но, процесс идет непросто, а многие действующие геополитики и «сильные мира сего» в попытках сохранить своё доминирование и, как следствие, однополярность мироустройства действуют в соответствии с теорией управляемого хаоса применительно к международным отношениям. В связи с проведением военной операции в Украине министр иностранных дел России С.В. Лавров отметил: «Решаемый вопрос не столько про Украину, сколько про миропорядок – это смена эпох». И на этом фоне против России и Союзного Государства в целом развязана гибридная глобальная война, а в рамках её проведения используется весь консолидированный информационно-пропагандистский ресурс потерявшего человеческий облик Запада.

Объектом такого рода информационных атак и специально спроектированных фейков, носящих чудовищный характер (Буча, Краматорск и др.), является как, собственно, российская аудитория с целью мобилизации всех антигосударственных сил, так и население Европы прозападной ориентации, получающей только специально препарированную, искаженную информацию, в основе которой лежит пещерная русофобия. Совершенно очевидно, что вся эта иерархия модераторов от информации ставит своей целью тотальное обалванивание обывателя и возбуждение у него низменных чувств отвращения ко всему русскому, начиная с пересмотра роли СССР в победе во второй мировой войне (мем о русской агрессии и уравнивание Гитлера и Сталина) и заканчивая спортом, туризмом, культурой, литературой, образованием и т.д. Очевидно, что для борьбы с этой скоординированной информационной вакханалией необходимо создание эффективного механизма борьбы с фейковым наполнением СМИ и подменой реальных событий и процессов иллюзорными виртуальными образами надуманных и специально сконструированных «событий», несущих в явном виде деструктивную агрессивную энергию разрушения как индивидуального, так и массового сознания на уровне целых этносов и социумов.

Но и в это неспокойное время у нас есть очень важные поводы для общей радости! Наш общий праздник, а он отмечается со 2 апреля 1997 года — День единения народов Белоруссии и России. В эти майские дни 25 лет назад (2 апреля 1997) был подписан «Договор о Союзе Беларуси и России», а 23 мая 1997г. и Устав Союза. Т.е. нашему Союзному Государству 25 лет! Все эти годы несмотря на то, что у нашего общения для наших сердец никогда границ не было, нас, тем не менее, нас разделяли физические, торговые и прочие границы. Несмотря на общее Союзное Государство, каждое государство, по большому счёту, строило самостоятельно свою информационную безопасность (ИБ) от разработки национальных криптографических стандартов до правового регулирования и защиты контента своих СМИ. Порой за прошедшие годы возникало недопонимание действий друг друга, что выражалось в жестких журналистских демаршах, скорее направленных на желание прокопать глубокую и широкую борозду недоверия между нами, нежели возвести мосты братского единения и дружбы. Но теперь мы встречаемся в другом Союзном Государстве, которое, будем полагать, станет основой нового мощного по-настоящему единого государства. Конечно, нашим врагам, ведущим против нас подготовленную, хорошо спланированную тотальную гибридную войну, такой крутой поворот истории не нравиться. Они всячески стремятся его остановить или, хотя бы, затормозить. Но мир меняется стремительно на наших глазах! Происходят судьбоносные события не только на полях сражений в Украине, но и в нашей совместной жизни.

Так, в Москве 16 мая состоялся юбилейный саммит Организации Договора о коллективной безопасности (ОДКБ), посвященный 30-летию подписания Договора о коллективной

безопасности и 20-летию создания ОДКБ. Принято Заявление членов Совета коллективной безопасности.

В своём ярком выступлении на этой юбилейной встрече среди первоочередных шагов, направленных на укрепление ОДКБ в нынешней беспрецедентной ситуации глава Республики Беларусь А.Г.Лукашенко указал на: «**Необходимость повышения эффективности противодействия вызовам и угрозам в информационном пространстве, включая борьбу с фейками и дезинформацией».** Он отметил: «**Понятно, что против нас развернута сейчас гибридная война с составляющей частью, в которой основной является информационная война**. Для того, чтобы этому противостоять, **следует по максимуму использовать потенциал соглашения ОДКБ 2017 года о сотрудничестве в области информационной безопасности, активнее продвигать ОДКБ в социальных сетях, которые интенсивно используют наши западные оппоненты, с целью действенного реагирования на фейки и информационные вбросы**. Притом надо подумать серьезно и, может быть, пойти по пути Китая в информационной борьбе, особенно в интернете». Соответствующие задачи должны быть поставлены всем – внешнеполитическим ведомствам, спецслужбам и Секретариату ОДКБ.

Следует также отметить, что 20 мая с.г. на заседании Совета Безопасности Президент России Владимир Путин заявил, что **против Российской Федерации в киберпространстве развязали войну. На Российскую Федерацию наносятся чётко скоординированные кибератаки. Число кибератак на Россию выросло в разы**. «**Вызовы в этой сфере стали еще более острыми и серьёзными, более масштабными**». **Атаки наносятся из разных государств, при этом они четко скоординированы. По сути, это действия государственных структур**», – отметил Путин, напомнив, что в состав ряда армий некоторых стран официально входят кибервойска. В то же время, считает Президент РФ, **кибератрессия против страны, как и в целом «санкционный наскок», провалились.**

«В целом мы были готовы к этой атаке, и это результат той системной работы, которая велась все последние годы», – подчеркнул Путин.

Кроме того за время, прошедшее после нашей встречи год назад в Минске, 15 сентября 2021 года в Душанбе по результатам встречи министров иностранных дел ОДКБ было сделано совместное заявление о том, что государства – члены ОДКБ подчёркивают, что **трансграничный характер современных вызовов и угроз в сфере ИКТ диктует необходимость усиления координации дальнейших совместных мер в борьбе с использованием информационных критических технологий в террористических и других преступных целях**.

К важным вехам на пути создания коллективной информационной безопасности стран ОДКБ можно отнести принятие 19 ноября 2021 года в Санкт-Петербурге на заседании ПА ОДКБ **МЗ «Об информационной безопасности ОДКБ».** Исходя из понимания актуальности процессов цифровой трансформации и возникающих задач стратегического реагирования на новые вызовы и угрозы, в настоящем МЗ была предпринята попытка упредительного правового реагирования на них. Следует заключить, что в дальнейшем союзникам по ОДКБ предстоит предпринять шаги по обновлению и координации возможностей по осуществлению предупредительной стратегической коммуникации и оптимизации использования мониторинга для противодействия гибридным угрозам, включая разработку индикаторов, позволяющих оперативно прогнозировать и распознавать угрожающие ситуации в административно-политической, социально-экономической и культурно-мировозренческой сферах. Авторы модельного закона изначально руководствовались именно этими соображе-

ниями в условиях происходящих глобальных изменений в ходе цифровой трансформации всего мирового устройства. Конечно, не всё задуманное получилось, что закладывалось изначально, но шаг вперёд все-таки мы сделали! И дай Бог, ещё многое сделаем! Процесс работы над МЗ показал, что, к сожалению, не все страны ОДКБ разделяют необходимость в создании коллективной информационной безопасности ОДКБ. Представители Республики Казахстан (РК) заняли жесткую непримиримую позицию по неприемлемости ряда статей МЗ, в результате чего Закон был буквально уполовинен. И не случайно, что буквально через месяц в РК была предпринята попытка проведения цветной революции, которая благодаря волевому решению руководства ОДКБ была оперативно предотвращена. Но сам факт попытки её проведения не стал неожиданностью для нас.

В соответствии с Положением о сотрудничестве государств – членов ОДКБ, утверждённым решением от 10 декабря 2010 года, под системой информационной безопасности понимается комплекс мер правового, политического, организационного, кадрового, финансового, научно-технического и специального характера, нацеленных на обеспечение информационной безопасности государств – членов ОДКБ. Принятый МЗ и является поступательным движением вперёд в целях правовой реализации Стратегии коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года с учётом динамического развития глобального информационного пространства и кардинальных процессов повсеместной цифровизации базовых основ и общества, и государства.

Стало очевидно, и разработчики МЗ основывались на этом посыле, что **обеспечение ИБ любого государства-члена ОДКБ только в рамках своего национального законодательства уже НЕДОСТАТОЧНО (!), так как эти угрозы имеют трансграничный характер** в условиях новых вызовов и угроз. Мир, в котором мы живем, чрезвычайно изменился и, прежде всего, благодаря появлению новых сетевых информационных технологий осуществления трансграничных коммуникаций между народами и странами в едином глобальном информационном пространстве.

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

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

ряд Центров, предназначенных именно для коллективного взаимодействия в области обеспечения ИБ информационного пространства стран НАТО и не только в оборонительных целях.

Такой подход, на наш взгляд, было бы целесообразным распространить и на наше Союзное Государство.

Это тем более актуально сейчас, когда практически настало время передела мира. Однополярная система мироустройства безвозвратно уходит в прошлое. Однако коллективный Запад ведет ожесточенную борьбу за сохранение своих позиций. В ход идут все средства, в том числе, в зоне ответственности ОДКБ. Как отметил президент Белоруссии Александр Лукашенко: «От бряцания оружием натовским у наших западных границ до развязанной против нас, в первую очередь против России и Беларуси, полномасштабной гибридной войны. НАТО агрессивно наращивает мускулы, затягивая к себе в сети уже нейтральных вчерашних — Финляндию и Швецию. Действует по принципу „кто не с нами, тот против нас“. Лицемерно продолжает декларировать свою оборонительную направленность. На этом фоне контрастом выглядит подлинно оборонительная и миролюбивая позиция Организации Договора о коллективной безопасности».

В настоящее время лидерами наших государств отмечается коренное изменение спектра угроз в рамках так называемой стратегии ведения гибридной войны, когда особое значение приобретают не столько потенциалы вооруженных сил, а возможности использования непрямых способов воздействия на противника. А именно, использования экономических, информационных, военно-политических, социокультурных инструментариев воздействия на потенциального противника. Новый вид гибридного стратегического неядерного сдерживания представляет собой осуществляемый по единому замыслу и плану комплекс мер в политической, военной, экономической, киберфизической, информационной и других сферах, направленных на убеждение другой стороны в невозможности достижения ею своих политических целей путем ведения обычной или гибридной войны, вследствие неотвратимой угрозы возмездия. Использование в таком качестве возможностей гибридной войны расширяет диапазон сил и средств, применяемых государством в современных конфликтах для сдерживания и принуждения строптивых соперников, не прибегая к оккупации территории.

«На фоне оголтелого санкционного прессинга со стороны консолидированного Запада постулат единства и солидарности срабатывает далеко не всегда!» — посетовал Лукашенко, отметив, что ОДКБ надо брать пример с Евросоюза, который действует монолитно и сплоченно. «Если бы мы сразу выступили единым фронтом, не было бы этих „адских“, как говорят, санкций», — заключил он.

Поэтому наводить порядок в нашем русском «цифровом доме», действительно, нужно. В нём должны быть хозяевами мы сами, а не западные корпорации со своей цензурой.

Развитие системы коллективной информационной безопасности Союзного государства и ОДКБ

Современные информационные платформы начинают всё больше и больше управлять коллективным сознанием социумов. Они становятся мощным и эффективным инструментом информационных войн.

На примере Беларуси два года назад мы впервые в истории наблюдали, как телеграмм-каналы, созданные вне страны, пытаются направлять людей на улицах и разъясняют им, как нужно бороться с властью в стране. Это феномен, который надо тщательно изучать.

2022 год можно по праву назвать годом масштабной информационной атаки на цифровой суверенитет России со стороны западных интернет-площадок. Google и YouTube, Facebook и другие гиганты массово блокировали аккаунты и сообщения российских СМИ, а также использовали наработанные на других информационных «полигонах» специальные когнитивные алгоритмы для манипуляции сознанием жителей нашей страны. На проблему обратил внимание президент Владимир Путин. Уже даны поручения по ограничению засилья IT-корпораций. Но война в самом разгаре.

Надо понимать, что всё началось не сейчас, после 24 февраля. Запад ведёт информационную войну против России практически сразу после того, когда понял, что Россия не смирилась с предписанными ей западными лекалами конструирования свободы и демократии в их понимании. При этом западные соцсети сами занимаются прямой цензурой в России. Ещё недавно YouTube блокировал видеозаписи с гимном России, так как у него якобы появился американский правообладатель. Перед этим все мы были свидетелями, как в социальных сетях развернулась атака на детей с призывами выходить на массовые акции протеста. А ранее YouTube заблокировал не только аккаунт-миллионник Царьграда, но и видео RT, канал AnnaNews и многие другие российские СМИ. Также и в Facebook откровенно прибегли к зачистке неугодного Западу информационного поля. Известно, например, что модерацией сообщений российских СМИ в Facebook занимается украинский портал StopFake, который работает на деньги активно продвигающего демократию в Европе Фонда Джорджа Сороса.

Теперь все мы сталкиваемся с новыми угрозами для мирного сосуществования наших народов. Это не только угрозы терроризма и экстремизма, которые сотрясают, к сожалению, мирную жизнь наших народов. Это и вошедшие в практику наших оппонентов гибридные технологии «управляемого хаоса», будь это COVID, ИГИЛ, «цветные революции» и другие инструменты геополитического влияния на шахматной доске современного миропорядка, которые запускают в новом формате угрозы мирному сосуществованию как отдельным государствам, так и всему мировому сообществу и, что особенно важно, нашему совместному проживанию в мирном, созидательном совместном постсоветском пространстве.

Важнейшие общественно-политические события 2020 года (выборы в Беларуси, Киргизия, Армяно-Азербайджанский конфликт, выборы в США) продемонстрировали, что информационные угрозы являются не только трансграничными, но они исходят от надгосударственных структур, по-сути, управляющих современным международным сетевым информационным пространством (Twitter, YouTube, Facebook, мессенджеры и др. инструменты информационных транснациональных коммуникаций), которые имеют возможность отключения от информационного общения и доступа к коммуникациям даже Президента США. Эти новые вызовы и угрозы могут быть реализованы относительно как отдельного государства, так и Союзного государства и всей коалиции государств-членов ОДКБ.

Приоритетным направлением совместной деятельности в рамках Союзного государства и ОДКБ должно стать **обеспечение коллективной способности своевременно вскрывать и парировать угрозы цветных революций, инспирированных западными спецслужбами, работать на опережение.** С этой целью в рамках совместной стратегии должны быть разработаны планы по подготовке к коллективному отражению угрозы и внедрены методы обмена информацией между союзниками и партнерами, предусмотрены совместные шаги по борьбе с финансированием цветных революций из третьих стран за пределами единого оборонно-политического пространства государств-участников ОДКБ.

Следует включить в число приоритетных проекты по адаптации оборонных возможностей ОДКБ для ответа на гибридные угрозы против одной из стран-членов ОДКБ или коалиции. Изучить возможности военного ответа на гибридные угрозы, для чего разработать соответствующую нормативно-правовую базу в рамках диалога и укрепления сотрудничества и координации по осведомленности о ситуации, стратегическим коммуникациям, кибербезопасности и предупреждению и реагированию на кризисы для противодействия гибридным угрозам.

Достижение стратегической цели обеспечения коллективной информационной безопасности Союзного государства осуществляется путем разработки и системной реализации комплекса взаимосвязанных политических, дипломатических, оборонных, экономических, информационных и иных мер, направленных на упреждение или снижение угроз коллективной информационной безопасности Союзного государства.

В области информационной безопасности:

- формирование системы коллективной информационной безопасности Союзного государства;
- развитие межгосударственного сотрудничества и укрепление межведомственной координации в сфере обеспечения информационной безопасности;
- совершенствование механизмов по противодействию угрозам в информационной сфере;
- проведение совместных мероприятий по противодействию и нейтрализации противоправной деятельности в информационно-телекоммуникационном пространстве Союзного государства;
- взаимодействие в вопросах обеспечения международной информационной безопасности;
- выработка согласованных правил взаимодействия в информационной сфере, продвижение их на международный уровень;
- создание условий и реализация совместных практических мероприятий, направленных на формирование основ скоординированной информационной политики в интересах Союзного государства.

В сфере противодействия современным, в том числе, комбинированным формам воздействия на Союзное государство с целью разрушения их государственности, дестабилизации внутриполитической ситуации или смены политических режимов будут осуществлены следующие действия:

- на основе изучения и анализа практики применения извне технологий так называемых «цветных революций» и «гибридных войн» разработка совместных мер и технологий противодействия им;
- формирование коллективной системы упреждения и реагирования на «гибридные», в том числе, информационные угрозы, использующие в качестве среды воздействия единое информационное пространство Союзного государства.

Наш общий долг: защитить наше великое объединенное прошлое, отстоять главные скрепляющие наше единство духовно-нравственные скрепы и создать надежную основу для доверия и дружбы для грядущих поколений!

Предложения по консолидации деятельности государственных и общественных структур в целях ещё более тесного сближения братских народов Беларуси и России в рамках Союзного государства

1. Парламентскому Собранию Союза Беларуси и России.
   1.1. Разработать и принять в кратчайший срок Закон «О коллективной информационной безопасности Союза Беларуси и России»

   (Предусмотреть в нем гармонизацию национальных законов в этой сфере; спектр общих угроз; зоны ответственности; систему оперативного реагирования на коллективные вызовы и угрозы в этой сфере).
2. Советам Безопасности Беларуси и России.
   2.1. Создать межгосударственную совместную рабочую группу Союза Беларуси и России по разработке «Концепции совместного реагирования на вызовы и угрозы информационной безопасности Союзного государства».
   2.2. Разработать и принять Стратегию совместных антисетевых действий в едином информационном пространстве Союзного государства».
3. Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры) и Министерству информации Республики Беларусь (Мининформ).
   3.1. Создать ТВ-канал Союзного государства под эгидой Парламентского Собрания Союза Беларуси и России.
   3.2. Создать интернет-ресурс «Наш Союз», на котором открыть молодежный портал творческих инициатив, стартапов, инновационных проектов, объединений по интересам, клубы исторической памяти, поисковиков и т.д.
   3.3. Проводить совместные фестивали песни и музыкального творчества помимо Витебска (год в России, год в Беларуси).
   3.4. Проводить форумы, в том числе, on-line, по восстановлению исторической памяти о тяжких испытаниях, которые прошли братские народы России, Белоруссии и Украины в годы ВОВ, включая рассмотрение вопросов:
      - организация совместного нераздельного БП 9 мая ежегодно
      - правда о геноциде славянских народов СССР;
      - обличение преступных организаций и подразделений СС из этнических добровольцев (прибалтов и УПА, украинцев-бандеровцев), творивших невиданные злодеяния на оккупированных территориях СССР.
4. Минобрнауки РФ и Министерству образования Республики Беларусь.

   Гармонизировать образовательные стандарты и программы в области ИБ (взаимная приемлемость дипломов, обмен студентами и аспирантами, стажировки преподавателей и др.).
5. Министерству спорта и туризма Республики Беларусь и Федеральному агентству по туризму (Ростуризм).

   Предусмотреть в совместных планах организационные формы и финансовое обеспечение развития историко-патриотического туризма, включающего:

- сохранение и восстановление всех видов памятников военной истории;
- создание историко-культурных центров, кружков, которые бы занимались подобными проектами;
- поддержка военно-исторических клубов, поисковых организаций;

- организация на постоянной основе военно-патриотических спортивных соревнований, военно-исторических реконструкций
- создание совместной цифровой площадки Союзного государства, где бы молодежь могла делиться интересными маршрутами, в том числе проходящих через Союзное государство;
- создать актуализированный цифровой контент, в том числе, для продвижения рекламы о туризме в Беларуси и России на внутреннем и мировом уровне и т.д.
- развивать в рамках Союзного государства тематику «Историко-патриотический туризм как эффективное средство воспитания детей и молодежи Союзного государства».

РОЛЬ ИДЕОЛОГИИ В ПОСТРОЕНИИ НАИБОЛЕЕ ЭФФЕКТИВНОЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

М.А.ЖДАНОВ
Национальный центр управления обороной РФ

Анализ последних событий показывает, как глобальные исторические процессы вновь вывели мировые центры силы к цивилизационному противостоянию. На переднем крае этой борьбы традиционно оказалась Российская Федерация с ее уникальной полиэтнической и многоконфессиональной парадигмой существования. Снова российский народ поставлен перед выбором потерять все и даже самого себя, либо одержать убедительную победу, безвозвратно изменив весь уклад существующего мирового порядка.

Вековая конфронтация Запада и Востока перешла в горячую фазу. В стремлении максимально ослабить Россию коллективный Запад развернул войну во всех сферах, в том числе экономической, политической и информационной, создал все условия для роста военной эскалации не только по всей Украине, но и за ее пределами в Европе. Кроме того, США открыто заявили о начале Холодной войны, демонстрируя решимость к сохранению стремительно утрачиваемой глобальной гегемонии.

С этой целью западные страны во главе с США в течение восьми лет занимались милитаризацией Украины, создали мощный военный кулак на Донбассе, чем вынудили Российскую Федерацию начать специальную военную операцию с целью обеспечения национальной безопасности и защиты русскоязычного населения.

При этом специальная военная операция и причины ее проведения обнажили людоедскую сущность носителей ценностей так называемой западной (англосаксонской) цивилизации, в основе которой лежит культ стяжательства, доминирования над другими народами и паразитирования. Внедрение в украинское общество националистической идеологии и использование Украины исключительно в своих корыстных целях в очередной раз доказывает ложность навязываемых Западом так называемых либеральных демократических ценностей.

Характерно, что коллективный Запад во главе с США действует строго в логике последовательно реализуемой концепции, суть и цели которой наиболее полно изложены в директиве 20/1 совета национальной безопасности США 1948 года, где Россия, независимо от формы правления, определена в качестве основной угрозы для американской стороны. В отношении ее США уже тогда поставили задачи более бескомпромиссные, чем даже в отношении милитаристской Японии и фашистской Германии в период Второй мировой войны. По мнению американских аналитиков, существование единого социокультурного и ценностного пространства, сформированного населяющими почти двумястами народами и народностями Советского Союза, несло прямую угрозу Западу.

Одним из основных инструментов для обеспечения развала такого единства являлось поощрение развития в Советском Союзе сепаратизма и радикального национализма, которые позволили бы возродить национальную жизнь прибалтийских и других народов. Особое внимание уделялось развитию украинского национализма при признании неоспоримости факта, что населения России и Украины являются одним народом с единой культурой и исторической судьбой.

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 Белоруссию, 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».

Кроме того, через Белоруссию, как и Россию проходит «Великий шелковый путь», делающий Китай богаче, а Европу обеспеченнее. Богатый Китай и сытая Европа, в свою очередь, не нужна западной финансово-политической элите, основная часть которых сосредоточена в настоящее время в Вашингтоне и Лондоне. Американцам нужно, чтобы в ситуации срежиссированного ими хаоса капитал бежал из Европы к ним.

На фоне проведения специальной военной операции ВС РФ по защите Донецкой и Луганской народных республик по решению Президента Российской Федерации и поддержанной подавляющим большинством населения ярко проявили и дискредитировали себя носители так называемых либеральных демократических ценностей, присоединившихся к западной антивоенной пропагандистской кампании.

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 разви-

тия государства и общества. Если проще высказаться, в период существования СССР эту задачу выполняла соответствующая целям развития государства идеология, пронизывающая все сферы жизнедеятельности.

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.

Ну чтобы успешно двигаться вперед, прежде всего необходимо понять наши преимущества, сформулировать наши долгосрочные цели и приоритеты. Это позволит иметь твердую и целостную позицию в современном мире, в том числе в отношении Запада и навязываемых им ценностей. Необходимо провести анализ: на чем строится их доминирование, в чем заключаются их цели, преимущества и уязвимости? Не сформулировав ответы на эти кажущиеся простыми вопросы, невозможно выстроить эффективную систему государственного управления и систему обеспечения национальной безопасности, в том числе и информационной.

Если просто сказать, то ценностями и целями славянских народов всегда было стремление человека к счастью, которое достигается через реализацию его творческого и созидательного потенциала прежде всего на благо общества. Товарно-хозяйственные отношения, уровень развития технологий при этом являются лишь средствами обеспечения наиболее эффективной модели целей, преимуществ, приоритетов и идеологических установок такого справедливого общества, в том числе счастья каждого индивида.

В такой системе, где приоритетом является защита интересов «семьи, рода, народа, государства», человек не загнан ложными ориентирами, а его ценность и положение справедливо определяется его личным вкладом в дело развития и защиты общества, к которому он принадлежит.

Эти базовые ценности в том или ином виде заложены в основу докторальных документов наших государств.

И именно наличие в Советском Союзе более привлекательной модели построения справедливого общества, а не коммунизм и не коммунистический строй как таковые, способствовали освобождению от колониального рабства и формированию независимых государств, в том числе, Китая, Индии, Кубы, значительного количества стран Юго-Восточной Азии, африканских стран и др. Поэтому и сейчас эти страны крайне заинтересованы в реализации продвигаемой России справедливой многополярной модели мироустройства, в которой будущее и развитие гарантировано всем народам.

И напротив: согласно ценностям западной цивилизации целью жизни является культ стяжательства, а мерилом успеха –способность обладать максимальным количеством материальных ценностей и богатств, а через них реализацией власти в отношении других народов и соплеменников, то есть мерилом успеха является способность безраздельного личного доминирования над другими членами сообщества. К процессу глобального управления и принятия решений допущен крайне узкий никому не подконтрольный слой так называемых финансово-политических элит, реализующих исключительно собственные интересы.

В этой системе координат, когда даже ближний воспринимается как конкурент, не удивительно, что люди других национальностей и рас просто отвергаются и воспринимаются как

недочеловеки, предназначенные как раз для использования в своей конкурентной борьбе за место под солнцем. Учитывая, что такому обществу чужды понятия альтруизма, жертвенности, искреннего братства и взаимопомощи, человек с детства погружается фактически в противоестественную гонку за выживание и находится в нескончаемом стрессе всю жизнь! В таком обществе счастье недостижимо, так как невозможно получить удовлетворение, работая зачастую на износ только в корыстных интересах, человек не может быть удовлетворен. А жадность, как и глупость, не имеют границ!

Вследствие все более твердой и последовательной позиции России и Белоруссии по отстаиванию своих национальных интересов как во внутренней, так и во внешней политике Западом в последнее время развернута беспрецедентная гибридная война против наших стран, одной из составных частей которой является введение информационной войны с использованием самых последних и передовых так называемых когнитивных технологий, направленных на установление контроля за ментальной сферой человеческой жизнедеятельности.

В том, что конечной целью военных действий является изменение суждений противника, нет ничего нового. Эта идея является вечной правдой о природе войны и зафиксирована еще китайским полководцем Чжанцин (Сунь-Цзы) в своем трактате «Искусство войны».

Революция в информационных технологиях позволила осуществлять манипуляции по установлению влияния над ментальной сферой человеческой жизнедеятельности в беспрецедентных масштабах, а переход к навязываемому Западом «новому технологическому укладу», обусловленному развитием, повсеместным внедрением и насаждением технологий искусственного интеллекта, обеспечил возможность вести против России, Белоруссии и других народов бывшего Советского Союза полномасштабную когнитивную войну. Это война нового типа, война идеологий и псевдоидеологий, стремящаяся подорвать доверие, лежащее в основе наших обществ.

Надо понимать, что так называемое доминирование западного общества основывается на комплексном использовании и продвижении своих ценностных установок во всех сферах жизнедеятельности человека через масс-культуру, технологии, науку, обосновывающую и продвигающую соответствующие теории, навязываемую форму хозяйствования в виде капиталистических отношений и многое другое. Некритично принимая и адаптируя их у себя, государства и народы фактически теряют свою субъектность, превращаясь в колонию для Запада.

При этом особое внимание США и их союзники уделяют поддержке и внедрению крупнейших высокотехнологичных компаний в государственную систему обеспечения информационной безопасности, которые активно воплощают в жизнь и продвигают в мировом информационном пространстве западные ценности.

Например, такие IT-гиганты как Palantir, Apple, Microsoft, IBM, Meta, T&T, осуществляют свою деятельность по сбору, хранению, обработке и преобразованию колоссальных объемов разнородной информации в отлаженном правовом поле. По сути, оказывая требуемое влияние на неограниченную аудиторию, они стали эффективным инструментом продвижения национальных интересов своих государств на международной арене. Важен тот факт, что они являются системообразующими государствоориентированными компаниями с частным финансированием. Очень показательным при этом является жесткое выполнение требований по отсутствию в руководстве компаний чиновников различного уровня и их родственников.

Разрабатываемые Западом с 2005 года по военному заказу NBIC-технологии (нано-технологии, био-технологии, информационные технологии, когнитивные технологии) направлены на формирование и реализацию нового уклада человека в технологическом мире.

Целью данной деятельности, принципы которой отфиксированы в знаменитой и знаковой работе Клауса Шваба 2015 года «Четвертая индустриальная революция», является технологическое порабощение человека посредством установления над ним тотального контроля от рождения до смерти, под предлогом улучшения его жизни.

При этом после присоединения Крыма к России в 2014 году, Западом во главе с США сделаны выводы, что сознание российских людей во многом продолжает базироваться на принципах и ценностях времен СССР и именно это позволяет до сих пор мобилизовать общество в кризисных ситуациях. Поэтому Запад усилил когнитивные воздействия, направленные на разрушение общих ценностей славянского мира, куда безусловно включены и украинцы, и белорусы, и значительная часть населения стран бывшего СССР.

В результате целенаправленного когнитивного воздействия, прежде всего на молодежь через соответствующие нарративы, формируется разрыв между поколениями, которые начинают думать и разговаривать фактически на разных языках.

Притягательность нарративизма для молодежи, не обладающей выстроенной системой ценностей и широтой знаний, состоит в том, что с помощью данного подхода можно легко объяснить любую самую тяжелую для восприятия действительность. Еще в Советском Союзе нарком просвещения А.Луначарский заметил, что «из маленького ребенка дошкольного возраста можно лепить, школьника-ребенка можно гнуть, юношу можно ломать, а взрослого только могила исправит».

По сути, взяв на вооружение приемы и методы геббельсовской пропаганды, направленной на формирование в сознании человека веры в навязываемый иллюзорный мир, США и их союзники с использованием технологий обработки больших данных и когнитивного воздействия смогли фрагментировать общество на множество антагонистически относящихся друг к другу подгрупп. К ним относятся террористические и экстремистские организации, секты, фанатские группы, игровые сообщества, ЛГБТ движения и множество других. Такая фрагментация общества уже не позволяет государству целенаправленно реализовывать свои национальные интересы и делает крайне уязвимым перед западной экспансией, что и доказали нынешние события на Украине.

В этой связи показателен опыт Китайской Народной Республики по обеспечению информационной безопасности страны. Китайское руководство пришло к выводу, что жизнедеятельность общества все более зависит от информационных технологий и алгоритмов, фактически подменяя ценности государства и человека. Таким образом, кто управляет алгоритмами, тот и управляет миром. При доминировании в настоящее время в данной области западных IT-компаний и технологий, китайское правительство выбрало единственный путь для защиты государственных и общественных интересов, введя с 1 марта 2021 года в действие закон «обуздания алгоритмов».

Также, в этом году руководство Китая сосредоточилось на чистке интернет-пространства и устранении нарушений в десяти сферах и видах деятельности:

1. *Прямые эфиры и короткие видео;*
2. *информационный контент в многоканальных сетях;*
3. *фейки;*
4. *интернет для несовершеннолетних в период летних каникул;*
5. *программное обеспечение;*

6. *интернет-коммуникации;*
7. *алгоритмы;*
8. *киберсреда в период празднования китайского нового года;*
9. *администрирование аккаунтов;*
10. *фальшивый трафик, черный пиар и платные комментарии.*

Результатом проделанной работы стала возможность обеспечения социальной, финансовой и психологической защиты граждан от манипулирования, монополий, дискриминации и фейков, что полностью соответствует национальной идеологии Китая.

При этом технологические гиганты КНР обязаны предоставлять правительству возможность государственного владения и ключевого влияния на принимаемые компаниями решения.

Также важно отметить, что китайские власти пошли уникальным, кардинально отличающимся от западного, путем развития сильного искусственного интеллекта, основанного на многовековой китайской философии. Истинные цели данного решения – грандиозные: создание технологичных агентов, обладающих уникальными качествами и характеристиками:

- *автономным восприятием, познанием, принятием решений, обучением, исполнением и возможностями социального сотрудничества, которые соответствуют* ***человеческим эмоциям***, ***этике*** *и* ***моральным ценностям***.
- *автономным сознанием и имеющим воззрения на мир, на жизнь и на систему ценностей,* ***способным понимать воззрения людей****;*
- *когнитивными фреймворками и математическими моделями, способными четко выразить три названные воззрения на математическом языке и позволяющих анализировать мыслительные процессы в их основе.*

Например, данные агенты должны понимать, что такое быть живым, стремиться к хорошей жизни, вести осмысленную жизнь. По сути, оцифровывая и интегрируя знания двух конфуцианских школ, объединяющих философию, гуманитарные и социальные науки – в Китае формируется идеологическая система национальных ценностей, отвечающая новому технологическому укладу общества.

При этом к защите своих интересов в информационном пространстве Китай, как и любая серьезная держава, подходит комплексно, развивая и средства активного воздействия, в том числе в области обороны. В 2016 году в Китае сформирован новый вид вооруженных сил – силы стратегической поддержки НОАК, решающий весь спектр задач «военного противоборства в информационной сфере» (в соответствии с китайской терминологией), как информационно – технического, так и информационно-психологического характера, с включением в его состав всех необходимых средств, в том числе и для действий в космическом пространстве.

Кроме того, в 2019 году главой Китая Си Цзиньпином официально объявлено о разработке военной концепции «интеллектуальной войны», основанной на использовании технологий искусственного интеллекта в целях установления контроля над волей противника и прежде всего лиц, принимающих решения. Реализацией разработки этой беспрецедентной инновационной концепции Пекин стремится достичь преимуществ над противником, аналогичных применению фашистами «теории блицкрига» во Второй мировой войне.

Таким образом, теория когнитивных войн и технологий искусственного интеллекта следует рассматривать в качестве инструментов для формирования необходимой модели мира, позволяющей заинтересантам управлять (владеть) миром в современных технологических социальных условиях с заделом на будущее.

К сожалению, в настоящее время информационное пространство, в том числе союзных государств не в полной мере защищено от деструктивного информационного воздействия Запада. И построение КНР своей комплексной системы обеспечения информационной безопасности государства, пронизанной идеями продвижения и защиты отвечающих интересам страны ценностей, возможно рассматривать как положительный пример для адаптации и использования нашими странами.

Таким образом, без определения задающих направление развития страны целей и соответствующих им идеологических концепций невозможно обеспечить успешное и долгосрочное развитие страны в качестве суверенного государства, а также успешную конкуренцию в мире, в том числе делает невозможным построение эффективных систем обеспечения национальной безопасности государства, общегосударственных систем поддержки принятия решений руководства и автоматизированных систем управления.

Примечательным на данном направлении является опыт наших партнеров по Союзному Государству, которыми уже в 2003 году введен в учебные программы высших учебных заведений курс «Основы идеологии белорусского государства». Одной из главных задач этого курса стала политическая социализация, формирование определенной политической культуры и подготовка молодых граждан к полноценному участию в жизни страны. При этом авторы учебных пособий четко разделяют артикулированную государственную идеологию и государственную идеологизацию, то есть навязывание государственной идеологии как единственно правильной.

Справочно.

Государственная идеология определяется как совокупность взглядов, идей, представлений о прошлом, настоящем и будущем государства. Она обосновывает избранный государством путь развития.

Потому сегодня нашим странам в условиях беспрецедентного давления западных государств очень важно совместно, взяв лучшее что у нас есть, фактически создать единую систему безопасности Союзного государства, которая могла бы обеспечить опережающее развитие славянского мира. Мы вместе должны сделать то, чего Запад боится более всего: предложить в том числе и миру альтернативный мировой проект, который будет более адекватен наступившей новой исторической эпохе и более привлекателен для народов мира, чем «инклюзивный капитализм». Прежде всего он должен быть направлен не на соперничество, а синергию цивилизационных проектов.

При этом не надо верить блефу Запада, уверяющему, что они уже победили. Это абсолютная неправда. В условиях тотального нарушения норм международного права и взятых обязательств со стороны США и их сателлитов большинство стран не поддерживает несправедливую англосаксонскую систему однополярного мира.

Так, Китай подтвердил готовность уйти от доллара в рамках российско-китайского товарооборота и выступил с резкой критикой идеи исключения России из «Большой двадцатки», назвав российскую сторону важной частью содружества двадцати стран. При этом Пекин призывает китайские компании в России воспользоваться экономическими возможностями, созданными западными санкциями, и «заполнить пустоту», образовавшуюся на российском рынке с внезапным уходом западных компаний.

Индия вопреки давлению со стороны Запада не собирается замещать возникший в мире дефицит зерна и отказываться от российских энергоносителей. То есть и здесь не оправдались надежды западных стран, связанные с тем, что именно Индия, являющаяся крупней-

шим производителей пшеницы в мире, заменит Украину, которая не может сейчас обеспечить продажу своего зерна.

Иран также четко озвучил, что в случае подписания СВПД Тегеран не намерен конкурировать с Москвой на нефтяном рынке.

За вычетом ближайших друзей и военных союзников США на Западе и в Восточной Азии, находящихся в полной зависимости от них, остальной мир поддерживать кампанию по изоляции России не желает. Более 30 стран, включая ряд африканских государств, при голосовании по резолюции Генеральной Ассамблеи ООН воздержались и осуждать Россию не стали. Ни одна африканская страна не поддержала санкции против России.

Даже являющиеся союзниками США Объединенные Арабские Эмираты воздержались при голосовании по резолюции, подготовленной США и осуждающей действия России на Украине, что вызвало «эффект домино» в арабском мире. Другие арабские государства также как один воздержались от осуждений действий Москвы. Кроме того, новый президент ОАЭ шейх Мохаммед бен Заид Аль-Нахайян назвал Россию своим «вторым домом».

Таким образом, налицо кризис и гибель западной цивилизации. Мир необратимо меняется и уже вовсе не Россия, а Запад все больше оказывается в изоляции на мировой арене. Но блефовать они будут до последнего, используя приемы и методы Геббельской пропаганды. Как это было и в 1945 году, когда 29 апреля, то есть за день до самоубийства Гитлера и полного краха их плана о тысячелетнем рейхе, в планируемом к выходу в тираж последнем номере берлинской газеты сообщалось об успехах «немецкой машины» с тем, чтобы население страны верило в перелом и победу Германии.

Еще никогда Запад не был в таком невыгодном положении. Созданный западными глобалистами мировой порядок спровоцировал нарастающие ресурсный и продовольственный кризисы, обнажил его критические уязвимости и обеспечил России и ее союзникам неоспоримые преимущества. Таким образом, кризис на Украине следует рассматривать как исторический шанс для России и Белоруссии обрести полную самостоятельность в определении пути своего развития на благо наших народов.

«Есть нечто более сильное,
чем все на свете войска, –
это идея, время которой пришло»
(Виктор Гюго)

УДК 004.056

ЗАЩИТА ИНФОРМАЦИИ В УСЛОВИЯХ САНКЦИЙ

О.Ю. КОНДРАХИН

Научно-производственное республиканское унитарное предприятие
«Научно-исследовательский институт технической защиты информации»,
г. Минск, 220088, Республика Беларусь

Непрерывное развитие информационных технологий, разработка и внедрение телекоммуникационного оборудования, совершенствование возможностей технических средств,

используемых злоумышленниками для нанесения ущерба информационным ресурсам и системам, приводит к необходимости постоянного совершенствования, модернизации систем защиты информации. Вопросы информационной безопасности приобретают геополитический ракурс, а средства защиты информации становятся инструментами противодействия политическим решениям.

Последствия пандемии, вызвавшие дефицит полупроводников материалов, серверного, телекоммуникационного оборудования и увеличения сроков поставки оборудования в страну, вслед столкнуло большинство организаций с масштабными санкциями и уходом, приостановлением деятельности на российском и белорусском ИТ-рынке ряда ведущих зарубежных вендоров. Зарубежные компании, продукцией которых обеспечивалась защита информации, из-за введённых санкций отозвали лицензии, в том числе отключив обновления своих решений. В ряде случаев лицензии, выпущенные на ранее приобретенные зарубежные средства защиты информации, продолжают действовать, но с обновлениями могут возникнуть проблемы в части баз сигнатур антивирусной защиты, систем обнаружения и предотвращения вторжений. Кибератаки стали происходить гораздо чаще. Количество подозрений на инциденты информационной безопасности, фиксируемых SOC, увеличились на порядок. Обязательной мерой надежной защиты ИТ-инфраструктуры является сканирование на уязвимости. Однако нет ни каких гарантий, что доступ к международным базам данных общеизвестных уязвимостей информационной безопасности «CVE» (Common Vulnerabilities and Exposures) не будет завтра ограничен. Следует отметить, что региональные представительства не всегда спешат оперативно решать потребности заказчиков и занимают выжидательную позицию. Возможно зарубежные партнеры прорабатывают новые сценарии поставок – например через страны Таможенного союза, которые не попали под санкции.

Уход таких зарубежных вендоров как Cisco, Fortinet, Symantec, McAfee, PaloAlto создаёт потребность подбирать отечественные аналоги, в том числе и в области защиты информации. Чтобы помочь предприятиям и организациям в этом непростом деле, отечественные ресурсы предлагают соответствующие навигаторы по продуктам информационной безопасности, которые позволяют быстро подобрать близкие по функциональности замены для многих популярных зарубежных продуктов и решений, например, для следующих сегментов:

- защита периметра: взамен Cisco, PaloAlto, Fortinet (США) продукция CheckPoint (Израиль), Usergate (Россия);
- защита от целенаправленных атак: взамен Cisco, PaloAlto, Fortinet (США) продукция Checkpoint, Kaspersky, Positive Technologies;
- антивирусная защита, системы сбора и анализа информации о событиях безопасности (SIEM) взамен аналогично продукция Kaspersky, Dr.Web, Positive Technologies (Россия), ВирусБлокАда, Либрасофт (Беларусь).

Сегодня в каждом сегменте есть как российские, белорусские аналоги, так и зарубежные, но нет гарантий, что оставшиеся зарубежные компании не пойдут по политике отмены. В настоящее время можно с уверенностью сказать, что средств защиты информации в части прикладного программного обеспечения таких как SIEM, DLP, антивирусного программного обеспечения вполне предостаточно на ИТ-рынках России и Беларуси, в том числе сертифицированных в Республике Беларусь.

Использование продуктов Open Source в некоторых случаях позволяет преодолеть ограничения, связанные с санкциями и уходом западных вендоров, но тем не менее эти же

продукты (Open Source) выполняют требования санкционного законодательства, например, Open Source антивирус ClamAV, который выпускается под GPL-лицензией и принадлежит компании Cisco, стал недоступен для пользователей России.

Решения использования продуктов Open Source требуют дополнительных затрат в части:

совершенствования, модернизации прикладного программного обеспечения, разработки соответствующей документации, в том числе необходимости подтверждения в Национальной системе подтверждения соответствия Республики Беларусь требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY). Испытательная лаборатория государственного предприятия «НИИ ТЗИ» соответствует критериям Национальной системы аккредитации Республики Беларусь, аккредитована на соответствие требованиям ГОСТ ISO/IEC 17025-2019, что позволяет выполнять максимальный спектр оказываемых услуг в соответствии с действующими нормативными документами в рамках сертификации средств защиты информации (программных, программно-аппаратных и технических) на соответствие техническому регламенту Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY);

преднамеренная активация в программном и аппаратном обеспечении закладок различной природы и выполнение несанкционированных действий требует анализа исходного кода с целью выявления уязвимостей, ошибок, недекларированных возможностей, приводящих к компрометации информации, получению несанкционированного доступа или нарушению бизнес-процессов. Фиксируются случаи внедрения разработчиками программного обеспечения недокументированных возможностей, механизмов блокировки программного обеспечения.

Запланированный процесс импортозамещения выглядит разумно – отказ от зарубежных средств защиты информации, использование отечественных разработок, использование свободно распространяемого программного обеспечения. Однако при всем этом необходимо постепенно планировать процесс миграции на отечественные аналоги и обязательно по результатам пилотирования проектов. На разработку и тестирование необходимы колоссальные временные, финансовые и профессиональные ресурсы, а возможно и дорожная карта, учитывающая все подходы противодействия санкциям, рекомендации, направленные на снижение возможных угроз информационной безопасности, включая актуализацию законодательства и нормативных правовых актов в области информационной безопасности, развития средств защиты информации, сетевого телекоммуникационного оборудования, адаптации международных баз данных общеизвестных уязвимостей.

Основные рекомендации до этапа создания системы защиты информации должны содержать следующий ряд организационно-технических мер направленных на анализ перечня и инвентаризацию используемых:

- активов предприятия;
- внешних IP-адресов, подсетей, доменов, каналов управления администрирования средств защиты информации, сетевого коммутационного оборудования;
- информационных ресурсов, имеющих доступ из сети Интернет, в том числе открытых портов;
- средств защиты информации и телекоммуникационного оборудования;
- учетных записей пользователей и администраторов, в том числе для удаленного подключения сотрудников, организаций в рамках техподдержки;
- контроля групповых политик безопасности;

- уязвимостей по результатам внешней и внутренней проверке отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы, в том числе «пентестинг»;
- ограничение использования:
  - сетевых служб и сервисов, не задействованных в работе;
  - протоколов управления информационными ресурсами по результатам сканирования на уязвимости;
  - удаленного доступа к информационным ресурсам без использования средств криптографической защиты информации;
- требования идентификации и аутентификации, парольной политики;
- автоматизированный круглосуточный мониторинг событий информационной безопасности;
- резервное копирование;
- повышение квалификации.

Перспективы развития национальной системы кибербезопасности в Республике Беларусь.

В целях повышения уровня защиты национальной информационной инфраструктуры в Республике Беларусь будет создана национальная система обеспечения кибербезопасности, элементами которой будут:

Национальный центр мониторинга кибербезопасности и реагирования на киберинциденты;

Центры мониторинга кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры (владельцы КВОИ, уполномоченные поставщики хостинга, государственные органы и иные организации).

Основные задачи:

- постоянный мониторинг уязвимостей;
- анализ атак и вызванных инцидентов;
- минимизация последствий атак и восстановление информационной инфраструктуры;
- обеспечение взаимодействия по обнаружению, предотвращению и реагированию на инциденты информационной безопасности;
- оценка эффективности защиты информационной инфраструктуры;
- обучение.

Специалисты по информационной безопасности в данной ситуации имеют уникальную возможность кардинально улучшить позиции на ИТ-рынке, повысить уровень квалификации, внедрить свои продукты в самых разнообразных отраслях, получить обратную связь от большого количества новых пользователей, привлечь опытных экспертов, а также воспользоваться беспрецедентной поддержкой в рамках государственных программ.

УДК 629.01; 621.3.019.3

О НЕКОТОРЫХ АСПЕКТАХ И РЕЗУЛЬТАТАХ ИССЛЕДОВАНИЯ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ ПРОГРАММ СОЮЗНОГО ГОСУДАРСТВА ПО КОСМИЧЕСКОЙ ТЕМАТИКЕ

Г.В.КОРОВИН, А.Н.КОРОЛЕВ
«НИИ КС им. А.А. Максимова» – филиал АО «ГКНПЦ им. М.В. Хруничева»,
г. Королев, 141090, Российская Федерация

Введение

В теории информационного права вопросы информационной безопасности чаще всего связаны с вопросами защиты информации и свободы слова. В Союзном государстве информационная безопасность затрагивает сферу интересов личности, общества и государства. Опираясь на законодательное закрепление, под информационной безопасностью следует понимать «состояние защищенности страны и ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства ». Таким образом, Союзное государство в обеспечении целостности государств-участниц должно выполнять активные целенаправленные действия для формирования государственной политики в обеспечении информационной безопасности Беларуси и России, разработки целевых программ и предложений правового, методического, научно-технического и организационного обеспечения информационной безопасности (Рис.1.)

Рис.1 Информационная безопасность Союзного государства

На представителей высших органов власти Союза – Совет министров, Парламентское Собрание, Постоянный комитет – возлагается огромная ответственность, связанная с эффективным обеспечением управления информационными ресурсами. Во-первых, разработка и принятие нормативно-правовой базы, которая будет регулировать потоки информации в обществе. Во-вторых, разработка и принятие экономических методов, обеспечивающих информационную безопасность Союзного государства. Например, совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц. В-третьих, организационно-техническое обеспечение, которое заключается в мониторинге и контроле информационных ресурсов со стороны власти.

О космической деятельности в свете обеспечения информационной безопасности государства

Космическая деятельность затрагивает информационную, научно-техническую, оборонную сферы деятельности государства и напрямую участвует в обеспечении безопасности государства, в том числе в ее информационной составляющей.

Говорить о Союзном государстве, как о субъекте космической деятельности, видимо в настоящее время довольно преждевременно. Вместе с тем, даже с учетом разницы в космических научно-промышленных потенциалах России и Беларуси, уже длительное время наблюдается устойчивая тенденция формирования эффективно действующей кооперации предприятий и организаций наших государств.

В Республике Беларусь правовое регулирование в данной области осуществляется в соответствии с Указом Президента Республики Беларусь от 22.12.2004 № 609 «О реализации государственной политики Республики Беларусь в области исследования и использования космического пространства в мирных целях».

В Российской Федерации правовое регулирование отношений в области космической деятельности регламентируется Законом о космической деятельности от 20 августа 1993 г. N 5663-I в редакции от 11.06.2021 № 170-ФЗ. Для целей этого Закона под космической деятельностью понимается любая деятельность, связанная с непосредственным проведением работ по исследованию и использованию космического пространства, включая Луну и другие небесные тела.

Есть и другое определение, в соответствии с которым космическая деятельность – любая деятельность, связанная с доступом в космос, непосредственно в космосе, через космос и из космоса для достижения определенных целей: политических, военных, экономических, информационных, экологических, коммерческих и т.д.

Таким образом, космическая деятельность имеет сложную многоуровневую структуру.

Анализ официальных документов и научных исследований по космической тематике позволяет выделить в системе целей космической деятельности следующие важнейшие мотивы космической деятельности:

- информационно-научные: стремление расширить масштабы фундаментальности научных исследований за счет проникновения в космос и таким путем содействовать получению новых научных знаний;
- военно-политические: намерение установить контроль над космическим пространством и развитием военно-политической обстановки в мире для обеспечения собственных национальных, политических и военных интересов;

- идейно-философские: желание обеспечить своему государству престиж политического и идеологического лидера в мировом сообществе;
- эмоционально-идеалистические: стремление удовлетворить свое любопытство, ответить на вызовы неизвестности, приблизить время создания поселений в космосе и на планетах;
- экономические: намерение создать новые рынки космических товаров и услуг, совершенствование некосмической экономики за счет использования достижений космонавтики;
- экологические: стремление установить постоянный контроль за состоянием окружающей среды с использованием различных космических систем и средств дистанционного зондирования Земли;
- информационные: желание создания единого информационного поля на основе совершенствования потенциала современных информационных технологий, включающего в себя космические средства сбора и распространения информации.

Информационные процессы лежат в основе практически всех явлений в природе и обществе. Поэтому рассмотрение и исследование космической деятельности целесообразно рассматривать с использованием информационного подхода, который помогает раскрыть сущность обеспечения информационной безопасности с использованием космических систем различного целевого назначения.

Таким образом, информационный подход – это метод научного познания объектов, процессов или явлений природы и общества, согласно которому в первую очередь выявляются и анализируются наиболее характерные информационные аспекты, определяющие функционирование и развитие изучаемых объектов.

За последние годы космонавтика добилась значительных результатов в области информатизации общества, основными из которых являются:

1. Обеспечены основные потребности общества в космической связи и ретрансляции программ теле- и радиовещания.
2. Создан научно-технический задел по космическим аппаратам дистанционного зондирования Земли, метеонаблюдениям, фундаментальным космическим исследованиям, способным удовлетворить потребности общества в необходимом объеме выполнять задачи оперативного контроля состояния территорий с использованием средств наблюдения космического базирования и проводить непрерывный анализ состояния природной среды.

   Например, использование космической информации позволяет: выявлять очаги крупных площадных пожаров; производить оценку состояния рек, водоемов, почв; производить наблюдение и анализ ледовой обстановки; оперативно осуществлять контроль состояния границы снеготаяния, отслеживать наличие крупных заторов, вскрытие рек и водохранилищ в периоды весенних паводков; определять возможный ущерб природной среде, наносимый стихийными бедствиями и неосмотрительной деятельностью человека и т.д.
3. Обеспечена работа международной спутниковой системы КОСПАС-САРСАТ, предназначенной для приема из любого района мира сигналов аварийных радиобуев, опознавания объектов, терпящих бедствие, автоматического определения по этим сигналам географических координат места аварии и оповещения о бедствии поисково-спасательных служб;

4. Расширен спектр услуг (по непрерывности и точности) по определению местоположения и скорости объектов с помощью глобальных навигационных систем GPS и ГЛОНАСС.

В настоящее время, и реалии сегодняшнего дня подтверждают этот тезис, успех военных действий на суше, в воздухе и на море, в равной степени, как и предотвращение войны, военно-политических кризисов или вооруженных конфликтов существенно зависят от эффективности использования космической информации и, соответственно, от степени защищенности (обеспечения защиты) получаемой и используемой космической информации.

Поэтому целью обеспечения информационной безопасности с использованием космических систем является, прежде всего, разработка и эффективное использование комплексной информационной системы сбора, хранения, обработки, преобразования, передачи и реализации полученной космической информации.

Об исследовании отдельных аспектов информационной безопасности в рамках программ Союзного государства по космической тематике

Сотрудничество России и Беларуси по освоению космического пространства в рамках совместных научно-технических программ Союзного государства успешно ведется уже более двадцати лет. Интеграция усилий в области разработки космических технологий является одним из важных и перспективных направлений научно-технического сотрудничества России и Беларуси и имеет целью эффективное развитие и совместное использование космического потенциала этих стран в интересах решения социально-экономических, оборонных и научных задач, стоящих перед участниками Договора о создании Союзного государства. (Рис.2).

В рамках реализации указанной цели НАН Беларуси и Роскосмос в период 1998-2022 годы разработали и успешно реализовали шесть научно-технических программ Союзного государства по космической тематике – «Космос-БР», «Космос-СГ», «Космос-НТ»,

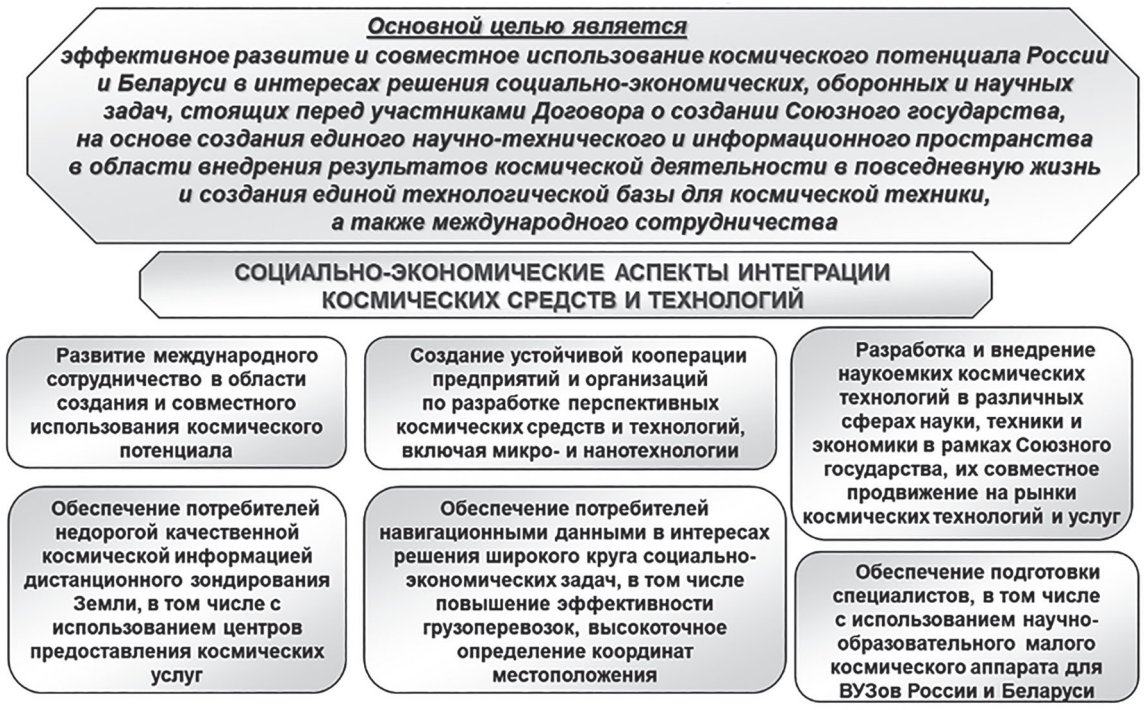


Рис. 2. Цели и задачи интеграции космических средств и технологий

«Нанотехнология-СГ», «Мониторинг-СГ», «Технология-СГ», реализация седьмой программы «Интеграция-СГ» завершается в 2023 году. В настоящее время установленную процедуру согласования и утверждения проходят две перспективные программы Союзного государства «Комплекс-СГ» и «Ресурс-СГ», реализация которых запланирована на период 2022-2027 годы. Периоды их выполнения условно разбиты на пять этапов (Рис.3).

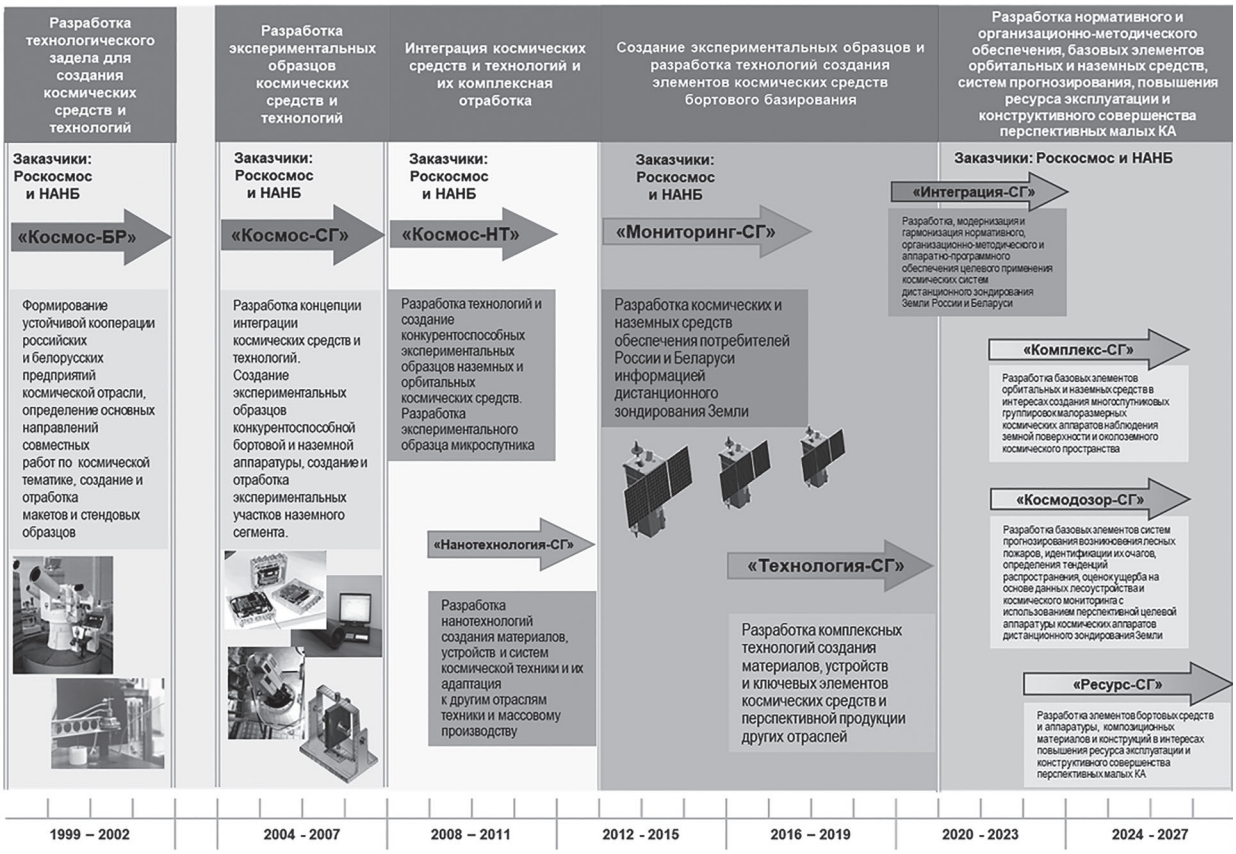


Рис. 3. Этапы выполнения программ Союзного государства по космической тематике

Результатами сотрудничества России и Беларуси, полученными при выполнении программ Союзного государства по космической тематике, стали, в том числе: экспериментальный образец унифицированной микроспутниковой платформы, десятки образцов маломассогабаритной служебной и специальной аппаратуры микроспутников нового поколения, экспериментальные образцы средств доведения и многоцелевой тематической обработки комплексной информации от средств космического наблюдения и наземного контроля, мобильные комплексы и станции приема данных от перспективных микроспутников и многое другое.

Полученный конструкторский и технологический задел по созданию маломассогабаритной космической аппаратуры позволил перейти к решению проблемы создания экспериментальных (технологических) образцов малоразмерного космического аппарата и наноспутников для отработки ключевых технологий функционирования многоспутниковых космических систем наблюдения поверхности Земли и околоземного космического пространства. Эту задачу планируется выполнить в рамках программы Союзного государства «Разработка базовых элементов орбитальных и наземных средств в интересах создания многоспутниковых группировок малоразмерных космических аппаратов наблюдения земной поверхности и околоземного космического пространства» («Комплекс-СГ»).

Выполнение работ, связанных с обеспечением информационной безопасности космической деятельности, осуществлялось и осуществляется, в основном, в течение двух последних этапов реализации Союзных программ в период 2015-2022 гг.

При этом основное внимание было уделено решению задач в трех основных областях обеспечения информационной безопасности при работе с космической информацией:

- при работе с данными ДЗЗ в территориально-распределенных системах (ТРС). Эту работу в рамках программы «Интеграция-СГ» выполняет АО «Российские космические системы»;
- при реализации облачных технологий хранения и обработки данных. Этим направлением работ занимается в рамках программы АО «Российские космические системы»;
- при обеспечении доступа к информации ДЗЗ на основе механизмов виртуальной станции приема данных ДЗЗ с использованием безопасных технологий хранения, обработки и представления информации. Эту работу также выполняет АО «НИИ точных приборов».

ТРС обеспечивает связь между поставщиками и пользователями информации ДЗЗ. Нарушений штатных режимов функционирования, вероятность сбоев или отказа аппаратно-программных средств, несанкционированный доступ пользователей к данным ДЗЗ, манипулирование этими данными и переадресация управления может привести к негативным последствиям. Основными направлениями обеспечения информационной безопасности в ТРС, которые реализуются в рамках программы Союзного государства «Интеграция-СГ», являются:

- защита данных методами криптографии (использование криптошлюзов);
- специальное тестирование ПО на отсутствие встроенных незапротоколированных функций;
- защита от несанкционированного доступа НСД (для определенных модулей системы). (Рис.4)

Наряду с преимуществами «облачных» технологий хранения и обработки данных ДЗЗ явным и существенным недостатком, сдерживающим их использование, является сложность обеспечения информационной безопасности. Опасность использования «облачных» технологий обуславливается относительно высокой вероятностью утечки, уничтожения, утраты, модифицирования информации, а также блокирования доступа к ней.

Основными проблемами обеспечения информационной безопасности при реализации «облачных» технологий являются:

- отсутствие контроля над процессами обработки информации;
- возможность утечки данных;
- возможность искажения или потери критически важной информации;
- возможность случайной публикации данных;
- влияние «облачных» вредоносных программ.

Решение задачи предотвращения неправомерных действий по отношению к информации и методам ее обработки возможно с использованием программного комплекса, обеспечивающего управление инцидентами информационной безопасности в реальном масштабе времени (рис 5).

Технология на основе механизмов виртуальной станции приема данных ДЗЗ (ВСПИ) развивается с целью сокращения времени доведения данных ДЗЗ и продуктов их обработки потребителям, обеспечения территориальной независимости от мест дислокации станций приема. Актуальной задачей при реализации технологии является формирование единого

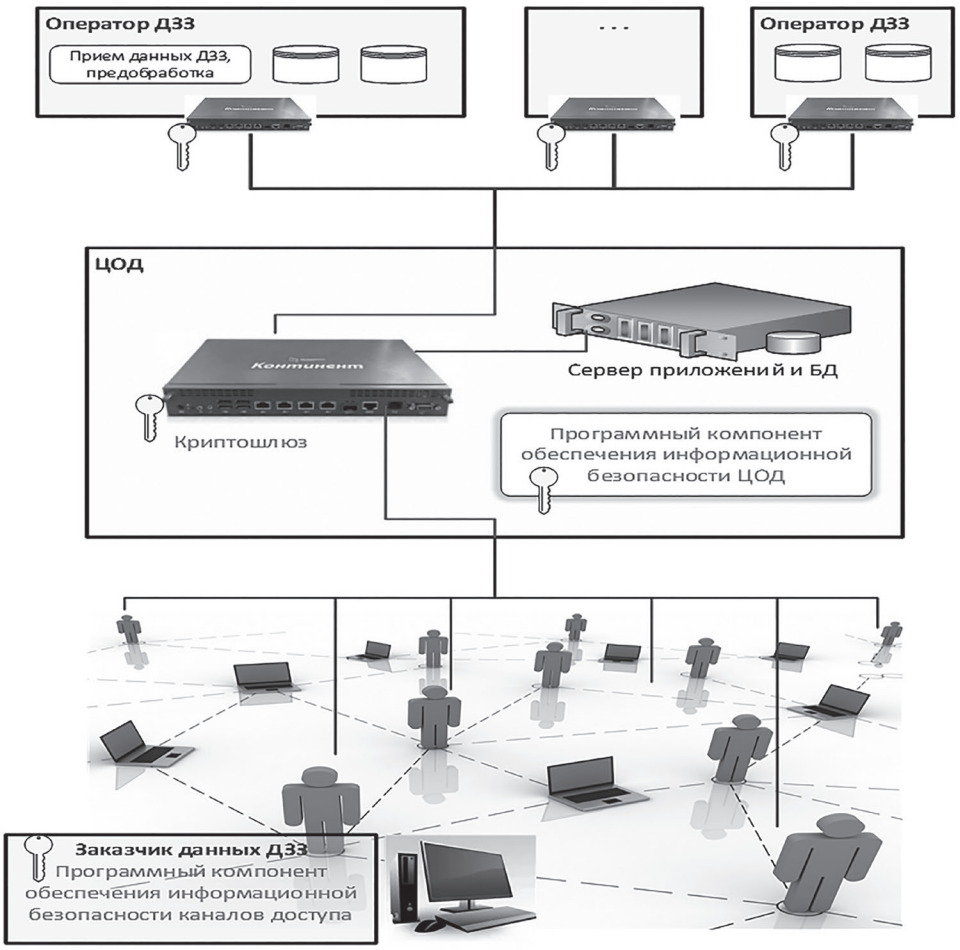


Рис. 4. Аппаратно-программный комплекс защиты информации ДЗЗ в территориально-распределенной системе

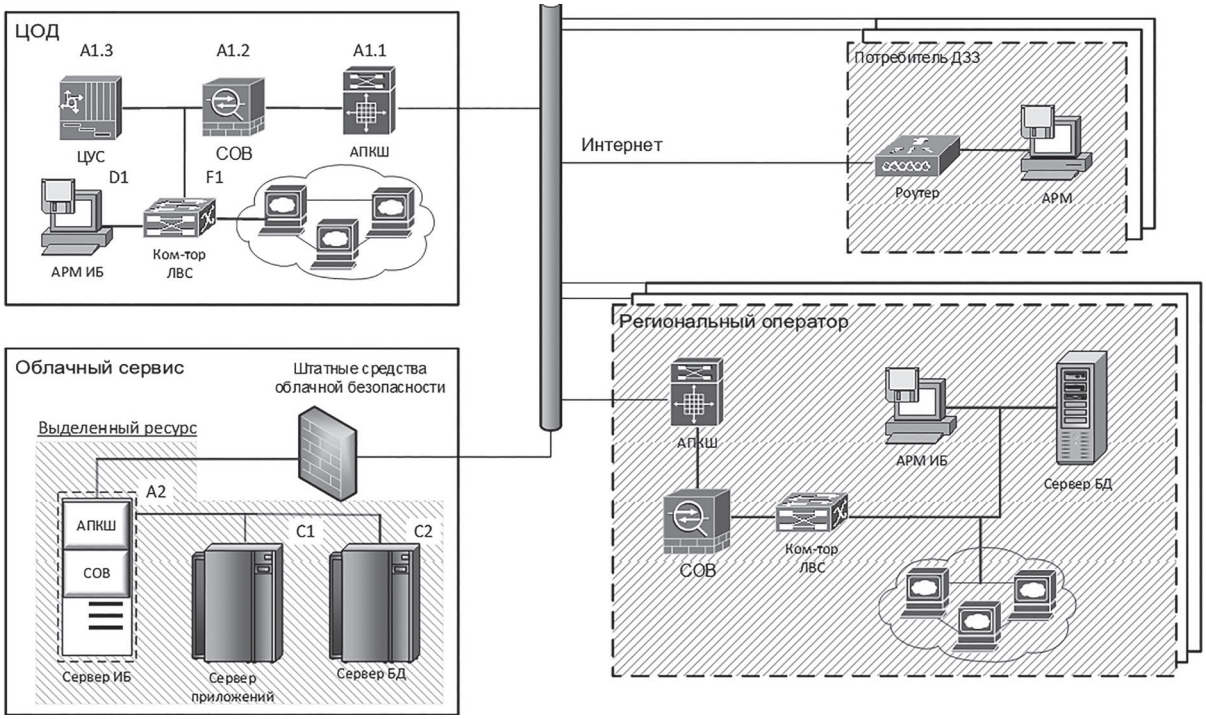


Рис. 5. Схема защиты информации с использованием «облачной» технологии

информационного пространства доступа поставщиков и потребителей к информации ДЗЗ с обеспечением заданного уровня безопасности. Потенциальную опасность представляют каналы передачи данных, процедуры запроса доступа к информации и системе в целом, несанкционированное изменение алгоритмов обработки данных (рис.6).

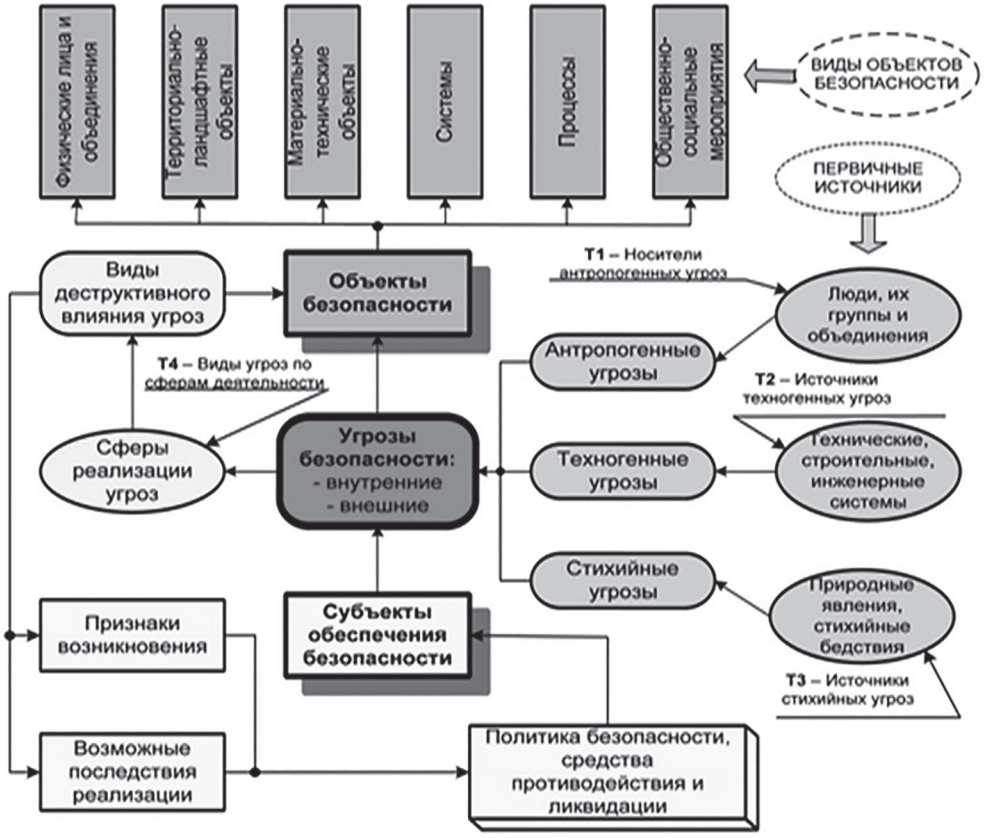


Рис.6. Базовая модель угроз безопасности при реализации ВСПИ

Особенности формата статьи не позволяют в полном объеме раскрыть полученные промежуточные результаты работ в части обеспечения информационной безопасности при работе с космической информацией. Поэтому ограничимся промежуточными результатами работ в части обеспечения информационной безопасности ТРС. Основными результатами этапа 2 СЧ НИР в части ТРС являются:

- проект типовой модели угроз и модели нарушителя системы обеспечения безопасности информации при работе с данными ДЗЗ в территориально-распределенных системах с учетом особенностей применения моделей как на территории Российской Федерации, так и на территории Республики Беларусь;
- технология обеспечения информационной безопасности при работе с данными ДЗЗ в ТРС;
- алгоритмы, реализующие предлагаемую технологию обеспечения информационной безопасности ТРС;
- предложения по оценке устойчивости системы обеспечения информационной безопасности при работе с данными ДЗЗ в территориально-распределенных системах;
- предложения по созданию стенда отработки и оценки устойчивости программного комплекса обеспечения информационной безопасности территориально-распределенных систем, техническая и программная документация на ЭО ПК ОИБ и стенд отработки ПК ОИБ.

Заключение

Применение программных средств, обеспечивающих повышение уровня информационной безопасности при работе с космической информацией, дает новые возможности и перспективы в области расширения международного рынка услуг ДЗЗ. Как территориально-распределенная структура Союзное государство предъявляет особые требования к информационному обеспечению данными ДЗЗ. Специфика заключается в необходимости параллельного обеспечения возможности функционирования сервиса услуг ДЗЗ в автономном режиме для составных частей единой ТРС и возможности глобального сервиса в интегрированном режиме.

Профиль современной системы информационной безопасности должен быть, прежде всего, бизнес-ориентированным. А это значит, что от традиционного подхода – обеспечения гарантированной защиты информации ДЗЗ надо отступать в сторону ее разумной защиты, взвешенно оценивая диктуемую обстоятельствами степень защищенности. Разрабатываемые технологии обеспечат безопасное использование веб-технологий, электронной переписки, межсетевого обмена данными ограниченного доступа, что позволит повысить эффективность информационной безопасности при работе с данными ДЗЗ в территориально-распределенной системе Союзного государства на 15-20% и даст возможность пользователям данного сервиса экономить на развертывании и поддержании своей собственной системы безопасности до 25 %.

Список литературы

1. Жук Е.И. Космическая деятельность и вопросы обеспечения информационной безопасности // ЭНТИ «Наука и образование», эл. № ФС77-30569, 2010. – 144с.
2. Общая теория национальной безопасности: Учебник // Под. общ. ред. А.А. Прохожева. – М.: РАГС, 2002. – 320 с.
3. Закон РФ «О космической деятельности от 20 августа 1993 г. N 5663-I в редакции от 11.06.2021 № 170-ФЗ.
4. Основы информационной безопасности: Учебное пособие // О.А.Акулов, Д.Н.Баданин, Е.И. Жук и др. – М.: Изд-во МГТУ им. Н.Э.Баумана, 2008. – 161 с.
5. Мысова Т.Ф. Информационная безопасность Союзного государства //Образование и право № 3 (55) – 4 (56), 2014 – 152 с.

УДК 004:34

КИБЕРПРЕСТУПНОСТЬ: СУЩНОСТЬ И СОДЕРЖАНИЕ

Д.Н. ЛАХТИКОВ
учреждение образования «Академия Министерства внутренних дел Республики Беларусь»,
220005, г. Минск, Республика Беларусь

В настоящее время на фоне активного развития науки и технологий, их внедрения в повседневную жизнь, сформировался новый вид преступности – киберпреступность. Это свидетельствует о том, что преступники достаточно оперативно используют результаты

научно-технического прогресса в своих целях. Данная тенденция представляет серьёзную угрозу общественным отношениям, складывающимся в информационной сфере, поскольку на данном этапе развития информационное пространство и общество уже неотделимы. Из-за своего междисциплинарного характера, специфической природы и повышенной социальной опасности киберпреступность, практически с момента своего появления и до настоящего времени является предметом исследования и дискуссий широкого круга специалистов: криминологов, криминалистов, специалистов в области информационной безопасности и защиты информации, – о понятии, природе, видах этих преступлений и мерах противодействиях им и др.

В свою очередь анализ состояния криминогенной ситуации за период с 2015 по 2021 г.г. свидетельствует о том, что более чем в 10 раз возрос удельный вес киберпреступлений. При этом, например, по подавляющему большинству (94,8 %, или 1149) уголовно наказуемых деяний против компьютерной безопасности (статьи 349 – 355 УК) лица, их совершившие, не установлены. Это обусловлено тем, что преступления данного вида, как правило, носят трансграничный характер и определенное их количество совершается иностранными гражданами либо с использованием интернет-ресурсов, компьютерных систем, находящихся за пределами Республики Беларусь.

В законодательстве Республики Беларусь фрагментарное определение термина «киберпреступление» содержится в пункте 8 Концепции информационной безопасности Республики Беларусь, утвержденной Постановлением Совета Безопасности Республики Беларусь от 18.03.2019 № 1 (далее – Концепция), однако не в качестве самостоятельного понятия, а составного элемента термина «преступления в информационной сфере». Анализ определения указывает, что под киберпреступностью понимаются преступления «против информационной безопасности (киберпреступления)». В свою очередь киберпреступность способна причинить вред различным охраняемым уголовным законом общественным отношениям, а не только отношениям в сфере информационной безопасности. Следовательно, не целесообразно определять киберпреступления по одному лишь объекту посягательства и просто выделить их в отдельную главу Уголовного кодекса. Также при формулировании определения необходимо учитывать, что термин «информационная безопасность» имеет более широкое значение и затрагивает, в том числе, контент сети Интернет, что не в полной мере соответствует общепринятым подходам при определении содержания понятия киберпреступность.

Одним из ключевых проблемных положений дискуссий относительно сущности и содержания рассматриваемого понятия является вопрос корреляции между киберпреступностью и традиционной преступностью. Ряд исследователей полагает, что, хотя киберпреступность может рассматриваться в качестве новой специфической формы преступности, она сохраняет сущностные признаки традиционной преступности, сущность данной формы преступности определяется через объект посягательства, и считают, что понятия киберпреступность и информационная преступность взаимозаменяемы. Между тем, следует предположить, что информационные преступления являются весьма широкой и неконкретной категория, которая охватывает значительный круг разнородных действий в информационной сфере.

Термин «киберпреступность» является общеупотребительным, как на бытовом, так и на законодательном уровне, в том числе и в научных кругах. Анализ научной литературы показывает, что в ряде работ можно встретить упоминание о киберпреступности, однако до настоящего времени ведутся многочисленные дискуссии о содержании и значении этого юридического понятия.

В международных актах не существует легальных дефиниций «киберпреступности» и «киберпреступления». Эти термины используются в 7 из 14 групп международных документов регионального характера. При этом их использование в названии, преамбуле и основной части документа не подкреплено нормативным определением данных категории в разделе, содержащем термины и понятия [1, с. 123].

В свою очередь в научной литературе сложились два подхода, касающиеся употребления термина «киберпреступность».

Сущность первого заключается в том, что использование термина «киберпреступность» для обозначения понятия, охватывающего преступные деяния, совершенные с помощью компьютерных устройств, информационно-коммуникационных технологий, не в полной мере оправдано. Так, В.Г. Степанов-Егиянц отмечает, что в целом, представляется целесообразным, с точки зрения семантики, необходимо отойти от «кибер»-терминологии и перейти к терминам, известным национальному праву, все известные явления и процессы, описываемые с помощью приставки «кибер», трансформировать в аналогичные явления, описываемые с помощью понятия «информация», «компьютер». Иначе говоря, понятие «киберпреступность» может быть без всяких потерь заменено на компьютерная преступность [2, с. 52]. При этом в настоящее время наряду с термином «киберпреступность» в научной литературе зачастую используются такие понятия, как, например, «преступность в сфере компьютерной информации», «преступления, совершаемые с использованием информационно-коммуникационных технологий».

В соответствии со вторым подходом понятие «киберпреступность» более полно отражает преступления в сфере компьютерной информации, а также преступления, совершенные с помощью компьютерных устройств, информационно-телекоммуникационных сетей и информационных технологий.

В научной литературе отсутствует единообразие мнений относительно определения сущности и содержания «киберпреступности». Можно обнаружить те же различия в подходах зарубежных и отечественных исследователей, что и в нормативных правовых источниках. Так, представители зарубежной науки в большинстве своем оперируют термином «киберпреступность» и связанными с ним понятиями с ключевой приставкой «кибер», это обусловлено тем, что проблема «киберпреступности» стала объектом научных исследований в зарубежных странах с 70-х годов прошлого века. Возникновение данного криминального явления, выявление и расследование преступлений потребовали разработки соответствующей теоретической базы, соответственно, именно зарубежные исследователи ввели данный термин в оборот в научных кругах [1, с. 129].

Термин «киберпреступность» в русскоязычный научный оборот пришел из англоязычной литературы, используясь для определения преступлений, совершенных в сети Интернет, либо с использованием информационно-телекоммуникационных сетей. Однако впоследствии средства массовой информации, позже и научное сообщество, перенесли указанный термин для обозначения совокупности всех видов компьютерных (информационных) преступлений. В английском языке «cyber» является не самостоятельным словом, а префиксом, то есть начальным элементом сложных слов, а на русский язык переводится как «связанный с компьютерами, информационными технологиями, «Интернетом». Между тем, что в Оксфордском толковом словаре приставка «cyber» определяется как «относящийся к информационным технологиям, сети Интернет, виртуальной реальности». В Кембриджском словаре указывается, что приставка «cyber» означает «включающий в себя использование компьютеров или относящийся к компьютерам, особенно к сети Интернет». Термины, обра-

зованные с приставкой «кибер» характеризуют понятия, связанные с деятельностью человека в виртуальном пространстве информационно-телекоммуникационных сетей, включая сеть Интернет, либо их использования в преступных целях. Кроме того, если обратиться к первоисточнику – иностранной терминологии – можно заметить, что за рубежом понятие «cybercrime» охватывает преступления, с использованием как глобальных компьютерных сетей, информационных технологий, так и компьютеров [3, с. 318].

Так, Т.Л. Тропина считает, что киберпреступность – это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей или компьютерных данных [4, с. 16]. Схожей позиции придерживается И.Г. Чекунов, предлагая рассматривать киберпреступность в качестве самостоятельного вида преступлений, определяемого на основе обнаружения обязательного присутствия в преступлениях таких признаков как средство или орудие, в качестве которых выступает вредоносное программное обеспечение или программно-техническое средство, подключенное к компьютерной сети или сотовому оператору связи [5, с. 182]. Понятие «киберпреступность» справедливо применять к совокупности преступлений, совершенных в пространстве информационных систем и информационно-телекоммуникационных сетей, либо с использованием информационно-телекоммуникационных сетей. Также в научной литературе употребляется понятие «Интернет-преступность», которое охватывается понятием «киберпреступность», т.к. глобальная сеть Интернет является лишь одной из многих информационно-телекоммуникационных сетей, которые могут быть использованы в противоправных целях.

В свою очередь, в качестве критерия, по которому то или иное преступление следует отнести к вышеназванной категории, отдельными авторами предлагается считать возможность совершения данного преступления без использования информационных технологий. Так, например, торговля оружием, может происходить как с использование информационных технологий, так и без них, в то время, как например, хищение имущества путем модификации компьютерной информации без использование информационных технологий невозможно.

Можно выделить отдельные недостатки при определении сущности и содержания киберпреступности различными авторами. Во-первых, несмотря на то, что информационное (кибер)пространство трансгранично, не все киберпреступления также носят трансграничный характер. Рассматривая такой признак киберпреступлений как использование вредоносного программного обеспечения можно отметить, чтио не все киберпреступления совершаются с его использованием. Такие признаки киберпреступлений являются факультативными и могут быть присущи отдельным киберпреступлениям. В отдельных случаях при определении понятия используется термин «компьютер», что позволяет акцентировать внимание на компьютерах как на объектах и средствах совершения данных преступлений. При этом темпы развития информационных технологий делают ограниченно применимым использование такого термина, что обусловлено тем, что в настоящее время уже само понятие «компьютер» становится размытым. Техническая составляющая киберпреступлений не сводится исключительно к применению компьютеров как технических средств, он может выступать своего рода орудием, своеобразным физическим объектом воплощения компьютерной системы (сети), в которой хранится информация.

Анализируя опыт Российской Федерации стоит отметить, что в законодательстве термины «киберпреступность» и «киберпреступление» не находят своего закрепления. Для

определения данного вида преступлений применяются понятия «преступления в сфере компьютерной информации», «информационные преступления», «преступления в сфере информационно-коммуникационных технологий, что отражается не только в национальном законодательстве, но и в международных документах, разрабатываемых и реализуемых по инициативе и при участии Российской Федерации: Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации 2001 г.; Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий 2018 г.; Соглашении о сотрудничестве в области обеспечения международной информационной безопасности, принятом Шанхайской организацией сотрудничества в 2010 г [1, с. 126].

Таким образом, не смотря на разнообразие подходов при определении сущности, содержания и определении понятия данного термина предлагается использовать его в следующем значении:

киберпреступность – это совокупность преступлений, предусмотренных Уголовным кодексом, при совершении которых нарушается состояние защищенности информационной инфраструктуры и содержащейся в ней информации.

Предложенное определение конкретизирует определение, содержащееся в Концепции и содержит устоявшуюся общепринятую терминологию, также закрепленную в Концепции. Данное определение раскрывает понятие «киберпреступность» через его признаки, а также не ограничено ни объектом посягательства, ни конкретной информационно-телекоммуникационной сетью, что делает его достаточно гибким. В свою очередь, с учетом специфического характера объекта, предмета и среды совершения киберпреступлений, любая норма и определение должны быть соотнесены с объективной возможностью практической реализации с учетом технических особенностей.

Список литературы

1. Старкова, Л. М. Подходы к пониманию и нормативному определению категории «киберпреступность» и смежных понятий в практике региональных международных организаций / Л. М. Старкова // Московский журнал международного права. – 2021. – № 4. – С. 123-135.
2. Степанов-Ягиянц, В.Г. Медодологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект) : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : диссертация на соискание ученой степени доктора юридических наук / Владимир Георгиевич Степанов-Ягиянц. – Москва, 2016. – 389 с.
3. Долженко, Н. И. К вопросу о содержательных аспектах киберпреступности / Н. И. Долженко, И. Г. Хмелевская // Nomothetika: Философия. Социология. Право. – 2020. – Т. 45. – № 2. – С. 315-322.
4. Тропина, Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : автореферат диссертации на соискание ученой степени кандидата юридических наук / Тропина Татьяна Львовна. – Владивосток, 2005. – 26 с.
5. Чекунов, И. Г. Киберпреступность: понятие, классификация, современные вызовы и угрозы / И. Г. Чекунов // Молодые ученые. – 2012. – № 3. – С. 178-186.

ДОВЕРЕННЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

ГЕОМЕТРИЧЕСКАЯ ИНТЕРПРЕТАЦИЯ МНОГОСЛОЙНОГО ПЕРЦЕПТРОНА С КУСОЧНО-ЛИНЕЙНЫМИ ФУНКЦИЯМИ АКТИВАЦИИ

А.П. КОВАЛЕНКО

Аналитическое агентство Gartner включило разработку интерпретируемого искусственного интеллекта (eXplainable AI, XAI) в первую десятку наиболее актуальных задач в области анализа больших данных [1]. Ожидается, что набор методов интерпретации обученной модели ИИ позволит объяснить ее поведение в каждом конкретном случае, выявить потенциальные ошибки, повысить прозрачность и надежность предлагаемых решений. Особенно это важно в областях с высокой стоимостью ошибки (управление беспилотными транспортными средствами, медицинская диагностика и т.п.). Недостаточное понимание пользователями процесса принятия решений моделями ИИ, например, нейросетями, которые обычно сравнивают с «черным ящиком», представляет собой серьезное препятствие их внедрения в бизнес и повседневную жизнь [2].

Ряд моделей ИИ (нейронные сети, машины опорных векторов, ансамбли решающих деревьев) считаются «плохо» интерпретируемыми (в отличие от «хорошо» интерпретируемых деревьев решений и линейной регрессии), хотя все происходящие внутри них вычисления известны. Здесь имеется в виду то, что процесс принятия решения не удается представить в «прозрачной» форме:

1. Показать, какие признаки входных данных существенно влияют, или наоборот, не влияют на решение.
2. Представить алгоритм принятия решения в виде понятных шагов.
3. Объяснить смысл промежуточных результатов вычислений.
4. Представить результаты обучения модели ИИ в удобной для восприятия форме (с привлечением средств визуализации).

Обзор методов интерпретации моделей ИИ можно найти, например, в [3].

Однако в некоторых частных случаях «плохо» интерпретируемая модель может быть преобразована в эквивалентную ей «прозрачную» модель без существенных затрат вычислительных и временных ресурсов.

В докладе представлен новый метод геометрической интерпретации результатов обучения многослойного перцептрона, основанный на преобразовании полносвязной многослойной сети с широко применяемыми кусочно-линейными функциями активации нейронов скрытых слоев (типа ReLU, LeakyReLU, ABS) в объясняющее двоичное дерево (eXplanatory Binary Tree, eXBTree).

Показано, что временная и пространственная сложность алгоритма построения eXBTree по обученной нейронной сети такого типа составляет $O(ndK)$, где n – объем обучающей выборки, d – размерность входного пространства, K – общее число нейронов во внутренних слоях сети.

Основываясь на результатах работы [4], сформулированы асимптотические условия, при которых двоичный классификатор на основе eXBTree является строго состоятельным при

увеличении объема обучающей выборки, то есть выборочная ошибка eXBTree-классификатора в пределе с вероятностью 1 совпадет с байесовской ошибкой.

В основе полученных результатов лежит тот факт, что многослойный перцептрон с кусочно-линейными функциями активации строит иерархическое (по слоям нейросети) рассечение компакта (например, гиперпараллепипеда) исходного d-мерного пространства, в котором решается задача нейросетевой аппроксимации функции, на выпуклые политопы (ячейки), формируя тем самым гистограмму, зависящую от данных.

Такая связь многослойного перцептрона с хорошо известным классификатором на основе гистограммной оценки плотности делает алгоритм нейросетевой классификации «прозрачным» как с содержательной, так и со статистической точек зрения. Однако, сразу возникает понятная для гистограммы, но «непрозрачная» для перцептрона проблема «проклятия размерности». В [4] показано, что число ячеек, на которое первый скрытый слой перцептрона рассекает гиперпараллепипед, пропорционально числу нейронов первого слоя в степени размерности пространства. Поскольку в современных нейросетевых моделях ИИ размерность пространства измеряется сотнями, а число нейронов в скрытых слоях достигает тысяч, получаемая «мегагистограмма» не сопоставима ни с каким объемом выборки! Поэтому ни о какой содержательной статистической постановке задачи нейросетевой классификации в общем случае речь идти не может.

Этот вывод означает, что нейросетевой классификатор решает задачу не статистической, а структурной классификации, особенности которой предполагается обсудить, с учетом сформулированных выше признаков «прозрачности», в завершение доклада.

Список литературы

1. https://www.gartner.com/smarterwithgartner/gartner-top-10-data-analytics-trends/
2. https://rb.ru/opinion/uzhe-ne-black-box/
3. Li et al., Interpretable Deep Learning: Interpretation, Interpretability, Trustworthiness, and Beyond, 2021, arXiv:2103.10689.
4. Devroye, L et al., A Probabilistic Theory of Pattern Recognition, Springer, 1996

УДК 004.838.2

ПРИКЛАДНОЕ ПРИМЕНЕНИЕ ДОВЕРЕННОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ ВНУТРЕННИХ ДЕЛ

И.А. КУБАСОВ
ФКУ «Научно-производственное объединение «Специальная техника и связь» Министерства внутренних дел Российской Федерации
г. Москва, 111024, Россия

В современных условиях применение искусственного интеллекта является одним из основных факторов экономического роста развитых государств и гарантированного обеспечения безопасности. Ведущие государства мира рассматривают широкомасштабное использование технологий искусственного интеллекта, как одно из ключевых направлений по достижению политического, экономического и военного лидерства.

Правительством Российской Федерации определен ряд высокотехнологичных направлений, так называемых сквозных технологий, которые обеспечат прорывную базу для национальной программы «Цифровая экономика Российской Федерации» [1]. В соответствии с Распоряжением Правительства РФ от 22.10.2021г. №2998-р «Стратегическое направление в области цифровой трансформации государственного управления» в ходе реализации стратегического направления в области цифровой трансформации государственного управления будут внедрены следующие технологии: искусственный интеллект; большие данные и интернет вещей [2].

Прикладное применение искусственного интеллекта, в том числе в сфере внутренних дел, позволяет не только автоматизировать любой сложности непрерывный процесс, но и настроить его в соответствии с конкретной задачей. Такое утверждение обосновано доказанной Джорджем Цыбенко еще в 1989 году универсальной теоремы аппроксимации о том, что искусственная нейронная сеть прямой связи с одним скрытым слоем может аппроксимировать любую непрерывную функцию многих переменных с любой точностью. Работа искусственного интеллекта становится более эффективной за счет постоянного обучения – чем больше искусственная нейросеть знает деталей конкретной задачи и потребностей, тем более высокая точность модели машинного обучения, что обеспечивает повышение эффективности управления.

Важно понимать, что искусственный интеллект, аккумулируя в себе совокупность прорывных достижений естественных и гуманитарных наук, становится новым фактором повышения эффективности государственного управления, в том числе органами внутренних дел Российской Федерации.

Стартовавшая цифровая трансформация МВД России, как переосмысление и глубокая реорганизация всех процессов управления с использованием цифровых инструментов, предполагает проведение фундаментальных и прикладных исследований в области искусственного интеллекта и анализа больших данных в сфере внутренних дел.

Среди основных планируемых результатов Ведомственной программы цифровой трансформации МВД России на 2022 – 2024 годы, в 2022 году – в рамках научно-исследовательских работ создание макетов программных средств и проектов технических заданий на опытно-конструкторские работы по внедрению технологий искусственного интеллекта. А в 2023 -2024 годах – выполнение ОКР «Создание информационной системы выявления признаков серийности (сходства) определенных категорий преступлений» и ОКР «Создание информационной системы определения индивидуальных фенотипических признаков человека на основе анализа биологического материала, изъятого с мест совершения преступлений» [3].

Чуть подробнее остановлюсь на втором проекте – определение индивидуальных фенотипических признаков человека на основе анализа ДНК.

Успехи в секвенировании генома человека и развитии технологий искусственного интеллект дали необходимые инструменты для анализа и выявления взаимосвязей фенотипических признаков человека с генетикой их наследуемости. Уже найдено принципиальное решение для определения по ДНК-маркерам принадлежность идентифицируемого индивида к определенной популяции населения и (или) определения географического региона происхождения его предков или родственников. Современные методы исследований ДНК позволяют также установить некоторые внешние признаки идентифицируемого неизвестного лица (цвет волос и глаз, пол, возраст) [4].

Так в 2021 году завершена пятилетняя научно-техническая программа Союзного государства «Разработка инновационных геногеографических и геномных технологий идентификации личности и индивидуальных особенностей человека на основе изучения генофондов регионов Союзного государства», разработанная Минобрнауки России совместно с Национальной академией наук Республики Беларусь в соответствии с постановлением Совета Министров Союзного государства от 16 июня 2017 г. № 26 (далее – НТП «ДНК-Идентификация») [5].

Целью НТП «ДНК-Идентификация» являлась разработка соответствующих мировому уровню развития науки отечественных унифицированных инновационных ДНК-технологий и методик для их применения в криминалистике, создание опытных образцов наборов реагентов для разработанных ДНК-технологий, а также проверка на практике инновационных геногеографических и геномных методик и ДНК-технологий, позволяющих повысить эффективность обеспечения безопасности граждан Союзного государства.

В рамках этой программы Институтом общей генетики им. Н.И. Вавилова РАН были разработаны технологии и наборы реагентов для определения этногеографического происхождения, возраста, цвета глаз и волос неизвестного индивида по его ДНК и сформированы базы данных генетических характеристик этнорегиональных групп для основных народов Союзного государства.

Разработанные методы определения этнорегиона происхождения включают определение Y-хромосомы. Y-хромосома присутствует только у мужчин и передается из поколения в поколение аналогично фамилии, от отца к сыну, что позволяет устанавливать дальнее генетическое родство по мужской линии. Так же как и для фамилий, для них имеется этническая специфичность. Сопоставление установленной конкретной линии с разнообразием и частотой мужских генетических линий в различных этнорегиональных группах позволяет определить, из какой группы происходит индивид.

Такой подход уже был успешно применен при раскрытии ряда преступлений, из которых наиболее известными являются установление преступника, совершившего теракт в аэропорту Домодедово в 2011 году, и установление личности новосибирского серийного педофила, который на протяжении десяти лет оставался неуловимым для следственных органов. Анализ ДНК указал на вероятный этнорегион происхождения преступника, что значительно сузило круг поиска и позволило установить его личность, менее чем за месяц [6].

Следует отметить, что создаваемые ведомственные системы искусственного интеллекта должны быть сопряжены с информационными системами заинтересованных федеральных органов исполнительной власти. Также потребуется предусмотреть внедрение искусственного интеллекта в защищенном исполнении в соответствии с национальным стандартом ГОСТ Р 52633.0-2006 «Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации» [7].

Результаты запланированных дальнейших НИОКР в сфере внутренних дел могут быть использованы с некоторыми доработками в деятельности Следственного комитета Российской Федерации, ФСБ России, Прокуратуры Российской Федерации, Росгвардии, ФСИН России.

Доверие к разрабатываемым системам искусственного интеллекта в сфере внутренних дел является важнейшим условием, определяющим возможность применения этих систем при решении ответственных задач обработки данных. Доверенный искусственный интеллект — это важная, интересная, многогранная тема. Разработчикам предстоит создать тех-

нологии, которым можно доверять в техническом (они должны быть надежны, устойчивы, безопасны) и психологическом плане.

В современных условиях применение технологий искусственного интеллекта неизбежно влечет проявление определенных рисков, основными из которых можно выделить:

- риски, связанные с иностранным происхождением систем искусственного интеллекта (наличие «закладок» и недокументированных функций, устаревшие и содержащие ошибки иностранные цифровые платформы, возможность несанкционированного доступа и утечки данных);
- технологические риски (невозможность контроля скрытых внутренних функций систем ИИ, построенных на многослойных искусственных нейросетях, низкая надёжность и риск выхода систем ИИ из-под контроля);
- риски мошенничества с данными и манипулирования ими (наличие целой индустрии по взлому/обману приложений ИИ, специализирующейся на биометрической идентификации);
- правовые риски (неурегулированность правового статуса ИИ, отсутствие нормативных правовых актов, определяющих ответственность за решения, принимаемые ИИ);
- кадровые риски (неумение технических специалистов донести до руководства соображения выгоды от внедрения ИИ; угроза пользователям ИИ или обслуживающему персоналу потерять работу/получить лишнюю нагрузку; использование неправильных алгоритмов и др.) [8].

Проблемы обеспечения безопасности ИИ приобретают всё большее значение по мере роста научного и общественного внимания к этому направлению технологического развития, особенно в современных условиях действия незаконных санкций недружественных стран.

В качестве основных проблем в сфере безопасности ИИ можно выделить:

- использование недостоверных или заведомо искаженных данных, применяемых для обучения алгоритмов ИИ;
- непреднамеренные ошибки и преднамеренная деструктивная модификация алгоритмов обработки данных в системах ИИ;
- необходимость применения доверенных аппаратно-программных средств для реализации алгоритмов ИИ;
- необходимость защиты ИИ от хакерских атак.

Вопросы обеспечения безопасности систем ИИ должны учитываться на всех этапах жизненного цикла – от первоначального проектирования и построения данных/модели до проверки и валидации, развертывания, эксплуатации и мониторинга.

Обеспечение безопасности систем искусственного интеллекта в целом включает в себя защиту как самих систем, так и цифровой инфраструктуры, в которой они функционируют. Когда компоненты с искусственным интеллектом подключены к большим организационно-техническим системам, уязвимости искусственного интеллекта (например, повышенное количество ложноположительных и ложноотрицательных решений при работе с большими объемами данных) будут наследоваться этими большими системами и приобретать, вследствие этого, более высокую или даже критическую значимость. По мере того, как возможности систем искусственного интеллекта продолжают расти, их сложность также будет возрастать, что делает более трудным подтверждение функциональности систем и конфиденциальности обрабатываемой информации. Соответственно, должны быть разработаны методы обеспечения безопасности и надежности создания, оценки, развертывания

и функционирования систем искусственного интеллекта, масштабируемые с возрастающими возможностями и сложностью систем.

Для нивелирования вышеперечисленных рисков необходимо отказываться от иностранных цифровых платформ, строить системы искусственного интеллекта на отечественных аппаратно-программных средствах, развивать научные исследования, разрабатывать нормативно-правовое обеспечение, а также готовить квалифицированные кадры в области искусственного интеллекта [8].

Для подготовки специалистов в области искусственного интеллекта целесообразно включить в учебные программы образовательных организаций дисциплину «Основы методов искусственного интеллекта» в качестве обязательного предмета, а также предусмотреть подготовку специалистов по дисциплине «Инженерия знаний». Узкоспециализированные модули (модели представления знаний, стратегия поиска в пространстве состояний, методы машинного обучения, методы планирования) должны коррелироваться с такими междисциплинарными программами, как прикладная математика, программирование, нейрофизиология, лингвистика и другими, обеспечивающими глубокое погружение в специфику конкретной области.

В заключении, отмечу, что система искусственного интеллекта должна быть доверенной, соответствовать ГОСТу Р 59276-2020 «Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения».

Доверие к системам искусственного интеллекта должно обеспечиваться:

- строгим выполнением законов, требований нормативно-технического регулирования, профессиональных руководств, инструкций и других утвержденных правил;
- обеспечением безопасности работы на техническом и инженерном уровне;
- этически корректным поведением на всех этапах создания и эксплуатации этих систем.

Список литературы

1. Паспорт федерального проекта «Искусственный интеллект» национальной программы «Цифровая экономика Российской Федерации». Утвержден протоколом заседания президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 23 октября 2020 г. №23.
2. Распоряжение Правительства РФ от 22.10.2021г. №2998-р «Стратегическое направление в области цифровой трансформации государственного управления».
3. Распоряжение МВД России №1/37 от 11.01.2022 «Об утверждении Ведомственной программы цифровой трансформации МВД России на 2022-2024 годы».
4. Отчет о научно-исследовательской работе «Формирование требований к проведению работ по разработке методов определения индивидуальных фенотипических признаков человека на основе анализа биологического материала, изъятого с мест совершения преступлений», шифр «Анатомия 1» / ФКУ НПО «СТиС» МВД России,– М., 2021. – 618 л. № госрегистрации 07218956.
5. Постановление Совета Министров Союзного государства от 16 июня 2017 г. №26 «О научно-технической программе Союзного государства «Разработка инновационных геногеографических и геномных технологий идентификации личности и индивидуальных особенностей человека на основе изучения генофондов регионов Союзного государства».
6. Боринская С.А., Балановский О.П., Курбатова О.Л., Янковский Н.К. По следам ДНК: как генетика народонаселения помогает криминалистике. Природа. 2020. № 11. С. 3–14.

7. Шапкин А.В., Кубасов И.А., Иванов А.И. Развитие отечественного нейросетевого искусственного интеллекта в защищенном исполнении. Вестник Воронежского института ФСИН России. 2019. № 4. С. 132-144.
8. Кубасов И.А. Проблемные вопросы применения технологий искусственного интеллекта в деятельности органов внутренних дел Российской Федерации. Вестник Воронежского института МВД России. 2021. № 3. С. 180-186.

УДК 003.26+004.032.26

О ПОДХОДАХ К РЕШЕНИЮ ЗАДАЧ КРИПТОЛОГИИ НА ОСНОВЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ И МАШИННОГО ОБУЧЕНИЯ

М.В. МАЛЬЦЕВ, Ю.С. ХАРИН
Учреждение Белорусского государственного университета
«Научно-исследовательский институт прикладных
проблем математики и информатики»
Минск, 220030, Республика Беларусь

Введение. Машинное обучение (machine learning) – сравнительно молодое направление анализа данных, включающее в себя методы и алгоритмы, которые позволяют автоматически выявлять закономерности в данных и затем использовать обнаруженные закономерности для решения различных задач: прогнозирования, классификации и кластеризации, обнаружения аномалий и т.д. [1]. Одним из наиболее перспективных и активно развивающихся методов машинного обучения являются искусственные нейронные сети (ИНС), широкое использование которых началось в 2005–2006 годах, когда канадские ученые Джеффри Хинтон и Йошуа Бенджи научились обучать так называемые глубокие нейронные сети [2]. Применение глубоких ИНС позволило значительно улучшить качество распознавания речи и изображений, существенно продвинуться в ряде задач биоинформатики, создать системы искусственного интеллекта, способные на сопоставимом с человеком уровне управлять автомобилем и играть в интеллектуальные игры. Закономерно, что интерес к ИНС как к эффективному инструменту решения самых разнообразных задач появился и в криптографическом сообществе. Применению ИНС и других методов машинного обучения в криптологии посвящена настоящая статья.

1. Машинное обучение и искусственные нейронные сети. Машинное обучение предполагает, что программа обучается по мере накопления опыта относительно некоторого класса задач T и целевой функции P, если качество решения этих задач (относительно P) улучшается с получением нового опыта [3]. Выделяют два основных класса задач машинного обучения: обучение с учителем (supervised learning) и обучение без учителя (unsupervised learning). Обучение с учителем подразумевает наличие множества обучающих данных (часто называемых размеченными), для которых известно значение целевой функции P (например, набор фотографий с отмеченными на них объектами), и задача состоит в том, чтобы, обучившись на размеченных данных, сделать вывод относительно новых (тестовых) данных (в нашем примере – выделить объекты на неразмеченных фотографиях). В задачах

обучения с учителем используются такие методы как деревья решений, метод ближайших соседей, логистическая регрессия, нейронные сети. В обучении без учителя размеченные данные отсутствуют, и задача, как правило, состоит в кластеризации – разделении данных на классы (число классов может быть как заранее заданным, так и неизвестным) в зависимости от определенных характеристик. Примером такой задачи является распределение программой-агрегатором новостей по тематическим рубрикам. В задачах обучения без учителя используются статистические алгоритмы кластеризации, метод главных компонент, нейронные сети.

Таким образом, важным методом машинного обучения, используемым как в задачах с учителем, так и без учителя, являются ИНС. Основным структурным элементом ИНС является перцептрон или нейрон (см. рис. 1). Перцептрон получает вектор входных значений $X = (x_1, ..., x_n) \in \mathrm{R}^n$ и вектор весов $W = (w_1, ..., w_n) \in \mathrm{R}^n$, соответствующих этим входным значениям. Выход перцептрона $y = y(X, W)$ имеет вид:

$$y = h\left(\sum_{i=1}^{n} w_i x_i\right),$$

где h – функция активации, в качестве которой чаще всего используются логический сигмоид, гиперболический тангенс, функция Хевисайда, функция ReLU (rectified linear units). Основной задачей при работе с нейронной сетью является ее обучение –определение вектора W, минимизирующего потери при обработке входных значений из заданного множества (например, функция потерь может определятся как суммарное расстояние между истинными значениями $y_0(X)$ и выходными значениями перцептрона $y(X, W)$.

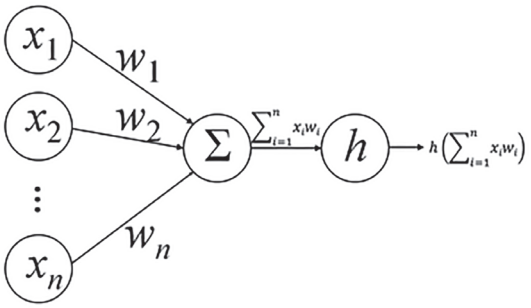


Рис. 1. Схема перцептрона

Возможности одного перцептрона сильно ограничены, поэтому их объединяют друг с другом (как правило, в слои) в нейронную сеть. На рисунке 2 приведена схема нейронной сети, в состав которой входят входной и выходной слои, а также m–2 скрытых слоя. В зависимости от строения (архитектуры) выделяют различные типы ИНС: сверточные сети, рекуррентные сети, генеративно-состязательные нейронные сети и другие [2]. Приведем далее кратное описание нескольких популярных архитектур ИНС.

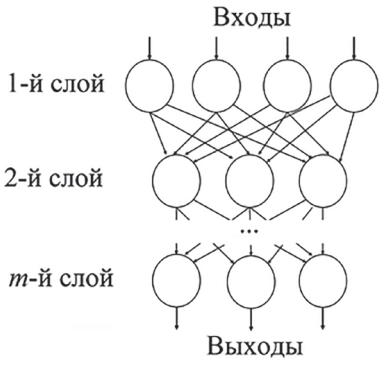


Рис. 2. Схема нейронной сети

Сверточные ИНС (convolutional neural network, CNN) предложены французским ученым в области искусственного интеллекта Яном ЛеКуном. Такие сети состоят из чередующихся слоев двух типов: сверточных (convolution) и субдискретизирующих (pooling). Сверточные ИНС широко применяются для распознавания изображений.

В рекуррентных ИНС (recurrent neural network, RNN) нейроны образуют направленную последовательность, вследствие чего такие сети могут обрабатывать серии событий во времени или последовательные пространственные данные. Такие сети используются для распознавания рукописного текста, распознавания речи.

Генеративно-состязательные нейронные сети (generative adversarial network, GAN), предложенны сотрудником компании Google Яном Гудфеллоу. В данной модели имеются две нейронные сети: генератор и дискриминатор. Генератор порождает объекты, принадлежащие различным классам, а дискриминатор пытается отличать объекты из разных классов. Применяются такие сети, например, для генерации и улучшения качества изображений.

2. Подходы к решению задач криптологии на основе искусственных нейронных сетей и машинного обучения. Идеи использовать машинное обучение в криптологии высказывались еще в начале 90-х годов Ривестом [4], но широкое распространение получили в последнее десятилетие вследствие развития методов обучения ИНС и роста вычислительных мощностей. ИНС, используя большие объемы информации, позволяют выявлять скрытые закономерности в данных сложной структуры, что способствует их применению в задачах криптоанализа [5–9]. Отметим, что в открытой печати, как правило, анализируются упрощенные версии криптографических алгоритмов: в работе [5] исследовалась упрощенная версия алгоритма DES, в работе [6] – алгоритм Speck32/64 с уменьшенным числом раундов. В работе [7] для восстановления бит ключа 6-раундовоого DES использовалась комбинация машинного обучения и методов дифференциального криптоанализа. В [8] исследовалась возможность применения методов машинного обучения для задачи различения шифртекста криптосистем DES, AES, RC4. В работе [9] – одной из первых, посвященных криптоанализу блочных шифров с помощью нейронных сетей, – исследовалась возможность восстановления ключа для криптосистем, основанных на сети Фейстеля. Рассматривался модельный n-раундовый шифр с длиной блока равной 16 битам. Атака состояла в переборе значений последнего раундового ключа с последующим обучением нейронной сети на множестве пар <открытый текст, шифртекст после n–1 раунда> для аппроксимации (n–1) раунда шифра. Для проверки правильности предположения о последнем раундовом ключе использовались тестовые данные: если предположение о значении последнего раундового ключа неверно, то обученная с таким ключом нейронная сеть на тестовых открытых текстах вместо верных шифртекстов выдаст случайную последовательность бит. Атака на основе предложенной ИНС позволила восстановить ключ 4-раундового шифра. Следует отметить недостаток, присущий многим рассмотренным статьям – недостаточная полнота описания архитектуры используемых нейронных сетей и условий проведения вычислительных экспериментов, что существенно затрудняет возможность воспроизведения приведенных результатов. Например, в работе [10] утверждается об успешном проведении криптоанализа DES и 3DES на основе 2048 и 4096 пар <открытый текст, шифртекст> (полученных на одном ключе) соответственно. Обучившись на указанных данных за сравнительное небольшое время (около 50 минут для DES и 70 минут для 3DES), 4-слойная нейронная сеть, по словам авторов [10], смогла успешно восстанавливать блоки открытого текста по блокам шифртекста без восстановления ключа. Подобные крайне оптимистичные результаты вызвали обоснованные сомнения и в работе [11] воспроизвести результаты из [10] не удалось.

Широко применяется машинное обучение в атаках по сторонним каналам, использующих особенности реализации криптосистем на физическом уровне. Для этих задач используются глубокие нейронные сети [12], метод опорных векторов [13], генеративно-состязательные нейронные сети [14].

В статье [15] предложен поточный шифр на основе нейронной сети, в [16, 17] нейронные сети применяются для анализа генераторов случайных числовых последовательностей. В статье сотрудников Google [18] построена состязательная нейронная сеть, в которой две стороны обучаются шифровать передаваемые друг другу сообщения по прослушиваемому каналу связи.

Методы на основе машинного обучения и нейронных сетей также применяются для анализа трафика. В работе [19] анализировался зашифрованный трафик, генерируемый различными мобильными приложениями: Facebook, Twitter, Dropbox, Gmail и др. с целью идентифицировать действие пользователя в приложении (отправка и открытие сообщения, публикация поста и др.). На рисунке 3 приведен фрагмент статьи [19], иллюстрирующий эффективность предложенного подхода для приложения Facebook.

Apps	Actions	Description	Precision	Recall	F-measure
Facebook	*send message*	send a direct message to a friend	1.00	1.00	1.00
	post user status	post a status on the user's wall	1.00	0.95	0.97
	open user profile	select user profile page from menu	0.96	0.91	0.94
	open message	select a conversation on messages	0.98	1.00	0.99
	status button	select "*write a post*" on user's wall	1.00	1.00	1.00
	post on wall	post a message on a friend's wall	1.00	0.98	0.99
	open facebook	open the Facebook app	1.00	1.00	1.00
	other facebook	other Facebook network traffic	0.99	1.00	0.99
	Average Facebook		0.99	0.98	0.99

Рис. 3. Результаты компьютерных экспериментов [19]

Машинное обучение используется и в стеганографии. Работы [20, 21] посвящены методам стегоанализа на основе нейронных сетей, в статьях [22, 23] ИНС применяются для встраивания секретной информации в контейнер. В [23] построены две глубокие ИНС для встраивания одного цветного изображения – секрета S в другое – контейнер C и последующего извлечения S из C, изображения S и C при этом имеют одинаковый размер. В разработанной системе стеганографической защиты информации встраивание информации может производиться в любые биты, а не только в наименее значимые, как во многих других стеганографических алгоритмах. Вследствие значительного процента информации, встраиваемой в контейнер, метод обладает недостатком – после восстановления в изображениях появляются искажения. На рисунке 4 представлен пример исходных изображений S и C, а также контейнера C' после встраивания в него S и восстановленного секрета S'.

Рис. 4. Пример работы ИНС [23]

В таблице 1 приведены значения ρ(*S, S'*) и ρ(*C, C*'), функция расстояния между изображениями ρ вычислялась как квадратный корень от усредненной по 1000 изображениям разности квадратов каждого пикселя (усредненная сумма квадратов разностей каждого из трех цветовых каналов). Функция ρ, таким образом, характеризует ошибку, вносимую в изображение алгоритмом встраивания, и изменяется от 0 до 255. Параметр β использовался при обучении нейронных сетей, функция ошибки *E=E*(*C*, *C*', *S*, *S*') для которых вычислялась по формуле: $E = \rho(C, C') + \beta\,\rho(S, S')$. Последняя строка в таблице соответствует случаю, когда встраивания в *C* не происходит.

β	ρ(C, C')	ρ(S, S')
0.75	0.75	3.6
1.00	3.0	3.2
1.25	6.4	2.8
0.00	0.1	–

Таблица 1 – Ошибки, вносимые алгоритмом [23]

Таким образом, машинное обучение и ИНС обладают высоким потенциалом для их применения в задачах криптологии и защиты информации – как за счет повышения эффективности существующих методов, так и путем создания на основе ИНС новых методов анализа.

Список литературы

1. Murphy, K. P. Machine Learning: a Probabilistic Perspective. – Cambridge University Press, 2013. – 1104 p.
2. Николенко, С. Глубокое обучение / С.Николенко, А.Кадурин, Е.Архангельская. – СПб.: Питер, 2018. – 480 с.
3. Mitchell, T. M. Machine Learning, 1 edition, New York, NY, USA: McGraw-Hill, Inc., 1997. – 414 p.
4. Rivest, R.L. Cryptography and machine learning / R.L.Rivest // Advances in Cryptology. ASIACRYPT 91. – 1991 – P. 427–439.
5. Danziger, M. Improved cryptanalysis combining differential and artificial neural network schemes / M. Danziger , M. Henriques // 2014 International telecommunications symposium (ITS), IEEE, 2014. – P. 1–5.
6. Gohr,A. Improving attacks on round-reduced speck32/64 using deep learning / A.Gohr // Advances in cryptology, CRYPTO-2019. – 2019. – P. 150—179.
7. Laskari,E. Cryptography and cryptanalysis through computational intelligence / E. Laskari, G. Meletiou, Y. Stamatiou, M. Vrahatis // Computational Intelligence in Information Assurance and Security, Springer. – 2007. – P. 1–49.
8. Chou, J. On the eectiveness of using state-of-the-art machine learning techniques to launch cryptographic distinguishing attacks / J. Chou, S. Lin, C. Cheng // Proceedings of the 5th ACM workshop on Security and articial intelligence, ACM. – 2012. – P 105–110. Albassal, A.M.B. Neural network based cryptanalysis of a Feistel type block cipher / A. M. B. Albassal, A. M. A. Wahdan // International Conference on Electrical, Electronic and Computer Engineering, 2004. ICEEC ‘04. – 2004. – P. 231–237.
9. 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.

10. Xiao, Ya et al. Neural Cryptanalysis: Metrics, Methodology, and Applications in CPS Ciphers. – 2019 IEEE Conference on Dependable and Secure Computing (DSC). –2019. – P. 1-8.
11. Lerman, L. Power analysis attack: an approach based on machine learning / L. Lerman, G. Bontempi, O. Markowitch // International Journal of Applied Cryptography, Vol 3(2). – 2014. – P 97–115.
12. Bartkewitz, T. Template Attacks Based on Probabilistic Multi-class Support Vector Machines / T. Bartkewitz, K. Lemke-Rust // Springer Berlin Heidelberg – 2013. – P.263–276.
13. Wang, P. Enhancing the Performance of Practical Profiling Side-Channel Attacks Using Conditional Generative Adversarial Networks / P. Wang, P. Chen, Z. Luo, G. Dong, M. Zheng, N. Yu, H. Hu. – 2020. – arXiv: 2007.05285.
14. Long, H. Stream Cipher Method Based on Neural Network / H.Long // Proceedings of the 2012 National Conference on Information Technology and Computer Science, CITCS. – 2012. – P. 414–417.
15. Melia-Segui, J. A Practical Implementation Attack on Weak Pseudorandom Number Generator Designs for EPC Gen2 Tags / J. Melia-Segui, J. Garcia-Alfaro, J. Herrera-Joancomarti // Wireless Personal Communications, Vol. 59. – 2011. – P.27-42.
16. Duy, N. Machine learning cryptanalysis of a quantum random number generator / N. Duy, J. Yan, S. Assad, P. Lam, O. Kavehei // IEEE Transactions on Information Forensics and Security, 14(2). – 2018.
17. Abadi, M. Learning to protect communications with adversarial neural cryptography / M. Abadi, D.G.Andersen. – 2016. – arXiv:1610.06918.
18. Conti, M. Analyzing android encrypted network traffic to identify user actions / M. Conti, L. V. Mancini, R. Spolaor, N. V. Verde // IEEE Transactions on Information Forensics and Security, Vol. 11, no. 1. – 2016. – P. 114– 125.
19. Qian, Y. Deep learning for steganalysis via convolutional neural networks / Y. Qian, J. Dong, W. Wang, T. Tan // SPIE/IS&T Electronic Imaging. International Society for Optics and Photonics, 2015.
20. Pibre, L. Deep learning is a good steganalysis tool when embedding key is reused for different images, even if there is a cover source mismatch / L.Pibre, J. Pasquet, D. Ienco, M. Chaumont // Electronic Imaging, 2016(8). – 2016 – P 1–11.
21. Jarušek, R. Neural network approach to image steganography techniques / R. Jarušek, E. Volna, M. Kotyrba // Mendel, Springer, 2015. – P. 317–327.
22. Baluja, S. Hiding images in plain sight: Deep steganography / S. Baluja // Advances in Neural Information Processing Systems 30. – 2017. – P. 2069– 2079.

УДК 004.056.53

СОВРЕМЕННЫЕ ТРЕНДЫ КОМПЬЮТЕРНОЙ ЛИНГВИСТИКИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

С. Ю. МЕЛЬНИКОВ, В.А. ПЕРЕСЫПКИН
ООО «Лингвистические и информационные технологии», г. Москва, 127018, Российская Федерация
ФГУП «НТЦ «Орион», г. Москва, 127018, Российская Федерация

Введение

Стратегические направления научных исследований в области обеспечения информационной безопасности перечислены в «Доктрине информационной безопасности Россий-

ской Федерации», утвержденной Указом Президента РФ № 646 от 5 декабря 2016 г. и в «Основных направлениях научных исследований в области обеспечения информационной безопасности Российской Федерации», утвержденными Секретарем Совета Безопасности Российской Федерации Н.П.Патрушевым 31 августа 2017 г.
Во многом эти направления связаны с развитием автоматических методов обработки информации, для чего необходимо совершенствовать, в том числе, вычислительно-лингвистические методы автоматической обработки текстов.

1. Задача коррекции искаженных текстов

Одной из сравнительно новых является задача коррекции искаженных текстов, полученных теми или иными системами машинного распознавания (речи, изображений текстов и др.). В последние годы эта задача формируется как отдельное направление (пост-обработка) и привлекает значительное внимание исследователей. В 2017 и 2019 гг. в рамках конференции International Conference on Document Analysis and Recognition (ICDAR) проводились соревнования различных систем коррекции текстов, полученных в результате оптического распознавания [1, 2]. В соревнованиях принимало участие более 30 участников, и если в 2017 году рассматривались тексты на двух языках (английский и французский), то в соревнованиях 2019 года к ним добавились болгарский, чешский, нидерландский, финский, немецкий, польский, испанский и словацкий языки. Близкие постановки рассматриваются также в биоинформационных задачах секвенирования и сборки больших геномов [3] для коррекции так называемых чтений, получаемых с помощью машин-секвенаторов.

Основным фактором, существенно затрудняющим понимание и перевод текстов, полученных при машинном распознавании речи или изображений текстов, в том числе в перспективных системах дополненной (виртуальной) реальности [4, 5], являются содержащиеся в них искажения в виде ошибочных символов, слов и словосочетаний [6, 7]. При значительном количестве искажений такие тексты становятся практически нечитаемыми.

В [8] показано, что орфографические ошибки в текстах патентов приводят к значительному ухудшению точности обработки поисковых запросов, и предложена специальная процедура обработки текстов патентов для повышения эффективности патентного поиска.

Специфические методы пост-обработки текстов, полученных в результате оптического распознавания, анализируются в [9]. Способы борьбы с искажениями текстов, которые возникают при наборе на клавиатуре, излагаются в [10] и [11].

Для моделирования искажений текстов предлагаются различные модели случайности. Так, в [12] рассматриваются следующие типы случайных искажений слов в тексте: бернуллиевский шум, гауссов шум, а также введенный авторами «состязательный» шум. Для повышения устойчивости в задаче классификации предложений предлагается обучение на текстах, подвергнутых рассмотренными искажениями рассмотренных типов. В [13] предложен способ моделирования искажений текстов, позволяющий получать искаженные тексты, близкие к тем, которые являются результатом работы систем распознавания. Способ использует взвешенную смесь случайных замен символов и случайных замен слов на близкие по расстоянию Левенштейна.

В [14] предложен многоэтапный метод коррекции искаженных текстов (в том числе, и сильно искаженных), основанный на последовательном определении ошибок и их исправлении. Отметим также возможность привлечения экспертов-лингвистов для объективиза-

ции и уточнения оценок качества работы автоматических систем обработки искаженных текстов [15].

2. Устойчивость языковых моделей к искажениям

В [16] для повышения устойчивости нейросетевых моделей к шумам предложены модификации схем вложения слов (words embedding) для следующих задач: классификация текстов, распознавание поименованных сущностей, извлечение аспектов. В [17] задача коррекции результата оптического распознавания рассматривается как задача перевода с одного языка на другой, и для нее применяется модель трансформера на уровне предложений. Достигнуто посимвольное улучшение точности распознавания на 29.4%.

Заметное влияние на исследования в области обработки текстов оказала работа [18], в которой показано, что символьные нейросетевые модели, которые используются для машинного перевода, как правило, не способны справляться ни с естественно возникающими искажениями в тексте, ни с искусственно внесенными. Рассмотрены четыре типа случайных искажений, связанных с перестановками букв внутри слова (1 – транспозиция соседних букв, 2 – случайное нарушение порядка следования букв в слове, за исключением первой и последней, 3 – случайная перестановка букв в пределах слова и 4 – случайная замена буквы на другую). Исследования проводились с текстами на французском, немецком и чешском языках, для оценки качества перевода использован показатель BLEU. Показано, что системе автоматического перевода Google Translate не удается переводить даже умеренно искаженные тексты, легко понимаемые человеком.

В [19] анализируется, как на точность машинного перевода влияет зашумленность обучающих данных. Рассмотрено несколько вариантов зашумления обучающих параллельных корпусов текстов. Показано, что нейросетевые системы автоматического перевода (NMT, Neural Machine Translation) менее устойчивы к зашумлению обучающих данных, чем системы автоматического перевода, построенные на статистических принципах (SMT, Statistical Machine Translation).

Предварительно обученные нейросетевые языковые модели, такие как BERT (Bidirectional Encoder Representations from Transformers, [20]) в настоящее время обеспечивают наивысшее качество решения многих задач в области вычислительной лингвистики, таких как аннотирование, распознавание поименованных сущностей, машинный перевод и др. В [21] рассматривается эффективность BERT в задачах анализа искаженных текстов. В качестве искажений выступают случайные опечатки, т.е. замена символа на другой символ, расположенный рядом на клавиатуре типа QWERTY. Рассматривался диапазон искажений от 0 до 22.5%. Показано, что с ростом уровня ошибок эффективность BERT резко падает. В частности, в задачах оценки тональности и определения близости предложений при уровне символьных ошибок в 15-17% результат сопоставим со случайным выбором возможных ответов. Авторы выдвигают предположение, что точность работы BERT может повыситься, если входные тексты перед точной настройкой BERT предварительно обработать системой коррекции ошибок. Другим вариантом решения этой проблемы может стать изменение архитектуры BERT для повышения его устойчивости к шуму.

В работах [22-24] отмечается, что современные нейросетевые методы машинного перевода неустойчивы к зашумлению текстов. Предложены подходы к искусственному зашумлению корректных текстов, которые бы обеспечивали их похожесть на некорректные тексты из социальных сетей и при использовании в качестве обучающих корпусов позволяли бы улучшить качество машинного перевода таких текстов.

Заключение

Проанализированы современные задачи автоматической обработки текстов, в интересах обеспечения информационной безопасности, для решения которых используются методы вычислительной лингвистики.

Список литературы

1. Chiron G., Doucet A., Coustaty M., Moreux J.P. ICDAR 2017 competition on post-OCR text correction // 2017 14th IAPR International Conference on Document Analysis and Recognition (ICDAR). 2017. Vol. 1. pp. 1423-1428.
2. Rigaud C., Doucet A., Coustaty M., Moreux J.P. ICDAR 2019 Competition on Post-OCR Text Correction // International Conference on Document Analysis and Recognition, pp. 1588-1593, 2019.
3. Das A.K., Goswami S., Lee K., Park S.J. A hybrid and scalable error correction algorithm for indel and substitution errors of long reads // BMC Genomics, v. 20(Suppl 11), pp.1-15, 2019.
4. www.topwar.ru > 18316 – pehotnaja-sistema-dopolnennoj-realnosti-IVAS (США). 29.03.2021.
5. www.tadviser.ru > index php / Статья Компьютерное_зрение_ технологии_рынок_перспективы. 26.06.2019.
6. Мещеряков Р.В. Структура систем синтеза и распознавания речи // Известия Томского политехн. ун-та. – 2009. – Т. 315, № 5. – С. 127-132.
7. Смирнов С.В. Корректировка ошибок оптического распознавания на основе рейтинго-ранговой модели текста // Труды СПИИРАН. – 2014. – Вып. 4. – № 35, С. 64–82.
8. Stein B., Hoppe D., Gollub T. The impact of spelling errors on patent search // In Proceedings of the 13th Conference of the European Chapter of the Association for Computational Linguistics (EACL 2012), pp. 570–579.
9. Nguyen T., Jatowt A., Coustaty M., Doucet A. Survey of Post-OCR Processing Approaches // ACM Comput. Surv. 54, 6, Article 124 (July 2021), 37 p.
10. Ghosh S., Kristensson P. Neural Networks for Text Correction and Completion in Keyboard Decoding // arXiv:1709.06429, 2017.
11. Рыбанов А.А., Филиппова Е.М., Свиридова О.В., Федотова Л.А. Система количественных показателей мониторинга за процессом развития навыка ввода информации // Педагогическая информатика. 2020. № 1. С. 136-142.
12. Zhang D., Yang Z. Word Embedding Perturbation for Sentence Classification // CoRR preprint arXiv:1804.08166, 2018.
13. Бирин Д.А., Мельников С.Ю., Пересыпкин В.А., Писарев И.А., Цопкало Н.Н. Об эффективности средств коррекции искаженных текстов в зависимости от характера искажений // Известия ЮФУ. Технические науки, № 8. — 2018. — С. 104–114.
14. Вахлаков Д.В., Мельников С. Ю., Пересыпкин В. А. Многоэтапный метод автоматической коррекции искаженных текстов // Известия ЮФУ. Технические науки, №7, 2020, С.35-45.
15. Германович А.В., Мельников С. Ю., Пересыпкин В. А., Сидоров Е. С., Цопкало Н. Н. Информационные измерения языка. Программная система оценки читаемости искаженных текстов // Известия ЮФУ. Технические науки, №8, 2019, С.6-18.
16. Malykh V. Robust-to-Noise Models in Natural Language Processing Tasks // Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics: Student Research Workshop, pp. 10–16, Florence, Italy, July 28 – August 2, 2019.
17. Soper E., Fujimoto S., Yu Y. BART for Post-Correction of OCR Newspaper Text // Proceedings of the 2021 EMNLP Workshop W-NUT: The 7th Workshop on Noisy User-generated Text, pp. 284–290, November 11, 2021.
18. Belinkov Y., Bisk Y. Synthetic and natural noise both break neural machine translation // arXiv:1711.02173, 2017.

19. Khayrallah H., Koehn P. On the Impact of Various Types of Noise on Neural Machine Translation // In Proceedings of the 2nd Workshop on Neural Machine Translation and Generation, pp. 74–83, 2018.
20. Devlin J., Chang M., Lee K., Toutanova K. BERT: Pre-training of deep bidirectional transformers for language understanding // arXiv:1810.04805, 2018.
21. Kumar A., Makhija P., Gupta A. Noisy Text Data: Achilles' Heel of BERT // Proceedings of the 2020 EMNLP Workshop W-NUT: The Sixth Workshop on Noisy User-generated Text, pp.16–21.
22. Vaibhav, Singh S., Stewart C., Neubig G. Improving Robustness of Machine Translation with Synthetic Noise // arXiv:1902.09508, 2019.
23. Niu X., Mathur P., Dinu G., Al-Onaizan Y. Evaluating Robustness to Input Perturbations for Neural Machine Translation // arXiv:2005.00580, 2020.
24. Karpukhin V., Levy O., Eisenstein J., Ghazvininejad M. Training on Synthetic Noise Improves Robustness to Natural Noise in Machine Translation // arXiv:1902.01509, 2019.

УДК 004.8

ПРОБЛЕМА ДОВЕРИЯ ТЕХНОЛОГИЙ КОМПЬЮТЕРНОГО ЗРЕНИЯ И СПОСОБЫ ЕЕ РЕШЕНИЯ

А.В. ФЕДОТОВ
Федеральное государственное унитарное предприятие «Главный радиочастотный центр» (ФГУП «ГРЧЦ»)
Москва, 117997, Российская Федерация

В связи с бурным развитием и внедрением во многие сферы повседневной жизни технологий искусственного интеллекта все актуальнее становится вопрос доверия этим технологиям.

По результатам **опроса «Доверяете ли Вы СИИ?»**, проведенного среди российских респондентов АНО «Национальные приоритеты» и ВЦИОМ, 48% ответили положительно. Это значительно превышает среднемировой уровень доверия, который составляет всего 28%.

Среди основных причин, по которым респонденты не доверяют ИИ – слабая развитость и изученность технологий, возможные сбои или ошибки в работе, незаменимость человека. И всего лишь 9% в качестве такой причины назвали угрозы безопасности/подверженности атакам. Но на наш взгляд, эта проблема гораздо важнее.

С этим согласны ведущие мировые ученые в области ИИ. По данным портала arxiv.org [1], **количество публикаций** по тематике атак на СИИ в научной литературе после первой обзорной статьи в 2018 году растет в экспоненциальной зависимости. Рассматриваются и классифицируются как способы атак, так и защиты от них, причем первые – гораздо более подробно.

На наш взгляд, **основными элементами доверенного искусственного интеллекта** являются:

- конфиденциальность: системы ИИ не должны допускать утечки данных;
- аудит и подотчетность: возможность оценки системы ИИ третьей стороной и, при необходимости, возложение ответственности за отказ систем ИИ, особенно в критических приложениях;

- безопасность и надежность: системы ИИ должны быть устойчивы к зашумлению входных данных и иметь возможность принимать безопасные решения;
- недискриминация и справедливость: системы ИИ должны избегать несправедливого предубеждения по отношению к определенным группам или лицам;
- объяснимость: системы ИИ должна быть в состоянии объяснять свои решения заинтересованным сторонам (которые должны быть в состоянии понять это объяснение).

Сегодня нейронные сети применяются в различных областях использования искусственного интеллекта, включая компьютерное зрение, обработку естественного языка и распознавание речи. При распознавании изображений сверточные нейронные сети могут классифицировать различные неизвестные изображения. При обработке естественного языка рекуррентные нейронные сети или сети долговременной памяти помогают переводить и обобщать текстовую информацию. При этом НС и их важная составляющая – глубокое обучение – имеют ряд уязвимостей, которые могут приводить к серьезным последствиям. Незначительные намеренные изменения в исходных данных или в работе сети порождают нераспознавание, утечку конфиденциальной информации или замедление работы систем ИИ. Эти атаки могут принимать различные формы и наносить удары по слабым местам в основных алгоритмах.

Основные **факторы риска,** которые заложены в СИИ – это непонимание и непредсказуемость действий алгоритмов; а также недостаточная устойчивость и надежность систем принятия решений.

Реализация этих рисков может привести к следующим **возможным угрозам** (в градации от наименьших последствий – к наибольшим):

- принятие СИИ и/или рекомендация неверных решений человеку;
- манипуляция общественным мнением, в том числе с использованием фейков (СМИ, социальные сети, рекомендательные сервисы); возможные сбои в работе фильтров контента, который блокирует размещение запрещенной информации в сети Интернет и позволит такой информации свободно распространяться;
- дискриминация людей по определенному признаку (например, системы скоринга, социального рейтинга и др.);
- выход СИИ из-под контроля и причинение вреда здоровья и жизни человеку (в сфере автотранспорта, здравоохранения, обороны и т.д.). Например, система ИИ автономного транспортного средства неправильно распознает знак остановки и причиняет вред другим транспортным средствам и/или пешеходам.

Все атаки на СИИ принято **делить по трем основным направлениям [2]**: в зависимости от информации о модели, которой обладает атакующий (черный, серый и белый ящики); в зависимости от направленности атаки (целевые, направленные на какую-то конкретную модель, и неизбирательные, ориентированные на широкий спектр моделей); и в зависимости от применимости (вирутальные, направленные только на данные в цифровой форме, и осуществимые в применимости к физическим объектам).

По типам атак на системы искусственного интеллекта в научной литературе рассматривается следующая классификация: «model extraction»/«data-free model extraction» (атаки извлечения модели с использованием и без использования данных); «model inversion» (атаки инверсии модели); «poisoning» (атаки отравления модели); «evasion» (атаки уклонения).

«Извлечение модели» предполагает дублирование модели машинного обучения через API, что не требует знаний обучающих данных и алгоритмов. Основной метод заключается в обучении замещающей модели. В итоге замещающая модель имеет аппроксимированные атрибуты и результаты прогнозов целевой модели. В данном случае целевая модель рассматривается в качестве «черного ящика» с неизвестными параметрами.

«Инверсия модели» [3] предполагает вывод из модели обучающих данных и восстановление принадлежности данных или свойств данных. Классический пример проиллюстрирован на слайде, когда в результате этой атаки на систему распознавания лиц было получено изображение лица человека, очень близкое к тому, что использовалось в обучающей выборке.

«Отравление» [4] предполагает искажение обучающих данных или искажение работы алгоритмов ИИ. Для воспроизведения интеллектуального поведения алгоритмам машинного обучения необходимы данные. Любое манипулирование данными, которое осталось вне поля зрения, может иметь катастрофические последствия или поставить под угрозу сам процесс обучения. Это возможно потому, что ИИ знает только определенные выученные шаблоны, которые соответствуют метке (например, под названием «знак остановки»). Таким образом, системы ИИ используют алгоритмы для извлечения и обобщения общих закономерностей в обучающих примерах.

В примере с распознаванием знака «стоп» алгоритм будет распознавать шаблоны, которые составляют это изображение – области красного цвета, формы букв и ряд других характеристик. Если шаблоны соответствуют изученным, то ИИ делает вывод о соответствии знаку остановки. Если же ИИ находит пример, который он ассоциирует с другим шаблоном, то ИИ сделает вывод в пользу этого шаблона.

Вместе с этим, «отравляющие» атаки на системы ИИ могут иметь цель скрыть информацию. Такие универсальные атаки отравляют распределение весовых коэффициентов в скрытых слоях нейронных сетей.

«Уклонение» [5] предполагает внесение «шумов» в обученные искусственные нейронные сети в целях нарушения корректности их работы. В случае, когда используется готовая нейросеть могут возникнуть непредвиденные проблемы. Добавляя определенный случайный «шум» во входящие данные за счет изменения весовых коэффициентов, нейросеть перестает распознавать объект, как один из знакомых. Например, нейронная сеть в беспилотном автомобиле при внесении «шума» в системы распознавания знаков ограничения скорости не распознает их как таковые. Такой тип уязвимости осуществляется при помощи другой нейронной сети, которая накладывает «шум» на целевую нейросеть.

На приведенной иллюстрации вносятся помехи в каждый пиксель изображения. Помехи рассчитываются однопроходными методами или методами итерации.

Представленные атаки также могут быть классифицированы **по уровню доступа к нейронной сети**. В частности, британская компания Roke Manor Research приводит в своем исследовании шесть уровней:

- «белый ящик» позволяет генерировать ложные входные данные и, соответственно, основывается на инсайдерской информации о модели, весах, скорости и методах обучения;

- «черный ящик» позволяет корректировать вредоносные входные данные на основе результата, генерируемого моделью;
- ограниченный «черный ящик» может осуществляться, если злоумышленники имеют доступ только к выходным данным модели;
- «черный ящик» с оценкой позволяют корректировать вредоносные входные данные на основе предварительных оценок нейроной сети, то есть злоумышленники имеют доступ к некоторым данным модели;
- замещение НС позволяет использовать замещающую нейронную сеть в качестве копии целевой нейронной сети. Этот метод обеспечивает разработку атаки любым методом и тестирование на замещающей сети для последующего использования на реальной сети;
- копирование НС представляет схожий вариант с замещающей НС, при которой замещающая сеть является аппроксимацией целевой сети и предполагает перенос вредоносных входных данных на алгоритм целевой сети.

При осуществлении описанных атак на нейронные сети могут использоваться **определенные методы.** В частности, исследователи выделяют:

- пиксельные атаки представляют злонамеренное изменение результата классификации изображения с его исходной метки на целевую метку. Изменение одного и/или нескольких пикселей приводит к неправильной классификации изображения;
- проективные искажения и аффинные искажения – это пространственные искажения, при которых сохраняются линии и параллельность, но не обязательно расстояние и углы;
- атаки на оптический поток – изменение передвижения объекта в кадре;
- вредоносная заплатка – это сгенерированный более характерный признак, который накладывается на изображение и приводит к неправильной классификации изображения. Здесь происходит изменение небольшого фрагмента данных таким образом, что сеть обращает внимание именно на него, а не на остальные данные;
- триггер – тип атаки, при котором вносятся незначительные изменения в данных, при встрече которого сеть будет реагировать определенным образом. Выявление триггеров в обученной модели практически невозможно;
- аудиоискажения и имитация речи другого человека применятся в системах распознавания речи. Инструменты синтеза речи на основе нейросетей высокоэффективны для введения в заблуждение современных систем распознавания говорящих (50–100% успеха). Синтетическая речь, созданная с использованием общедоступных систем, может обмануть как людей, так и программные системы. Кроме этого, аудиоискажения заключаются в встраивании неслышимых команд или повышения уровня шумов в окружении. Например, шум двигателя;
- энергоатака заставляет нейронные сети использовать больше вычислительных ресурсов, чем необходимо, и замедляет процесс «мышления» ИИ. То есть, при изменении входных данных можно изменять количество вычислений.

Приведем основные **технические методы защиты** от атак на СИИ. Можно разделить их на следующие основные категории:

Модификация модели

Состязательные атаки с искажениями и шумом: уменьшают ошибки классификации.

Защитная дистилляция: состязательный метод обучения, при котором целевая модель используется для обучения меньшей модели, которая демонстрирует более гладкую выходную поверхность.

Ансамблевое состязательное обучение: несколько классификаторов обучаются вместе и объединяются для повышения надежности.

Прочие: выработка устойчивости модели при обучении на стандартных данных, модели с квантованием.

Преобразование входа

Маскировка градиента: предотвращает использование злоумышленником полезного градиента.

Регуляризация ввода: используется, чтобы избежать больших градиентов на входе сети, которые делают сети уязвимыми.

Сжатие признаков: объединение выборок, которые соответствуют множеству различных векторов признаков в исходном пространстве, в одну выборку, что уменьшает пространство поиска, доступное злоумышленнику.

Кроме того, существует ряд стандартных методов, гарантирующие устойчивость целевой модели к известным атакам, а также комбинирование нескольких стратегий защиты и защиты от узконаправленных атак.

Говоря **об организационных методах защиты**, нельзя не отметить важность классических подходов к ИБ. Нельзя пренебрегать разработкой модели угроз и модели нарушителя для систем, использующих ИИ;

Кроме того, необходимо создать площадку для обмена лучшими практиками в области обеспечения доверия и безопасности систем, использующих ИИ, а также отечественную платформу для разработки и развития технологий ИИ(ОС, фреймворки, библиотеки, обучение и тестирование моделей и пр.).

Важно продолжать развитие процессов стандартизации ИИ и научных исследований в данной области.

В настоящее время во ФГУП “ГРЧЦ” ведутся работы по развертыванию экспериментального стенда для апробации основных типов и методов атак на СИИ, а также способов противодействия им.

В 2023 году ФГУП “ГРЧЦ” планирует разработать проект стандарта Предприятия, чтобы в пилотном режиме решить первоочередные вопросы обеспечения доверия и безопасности профильных для отрасли СИИ.

Надеемся, что в дальнейшем накопленный опыт и экспертиза позволят ФГУП “ГРЧЦ” участвовать в разработке национального стандарта доверия и безопасности СИИ в рамках механизма ТК 164 Искусственный интеллект.

Список литературы

1. 1. Naveed Akhtar, Ajmal Mian, Navid Kardan, Mubarak Shah. Advances in adversarial attacks and defenses in computer vision: A survey. [Электронный ресурс]. – 2021. – Режим доступа: https://arxiv.org/pdf/2108.00401.pdf. Дата доступа: 28.04.2022.

2. Maliamanis Theodoros, George Papakostas. Adversarial computer vision: a current snapshot. [Электронный ресурс]. – 2020. – Режим доступа: https://www.researchgate.net/publication/338957091_Adversarial_computer_vision_a_current_snapshot. Дата доступа: 28.04.2022.
3. Matt Fredrikson, Somesh Jha, Thomas Ristenpart. Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures. [Электронный ресурс]. – 2015. – Режим доступа: https://rist.tech.cornell.edu/papers/mi-ccs.pdf. Дата доступа: 28.04.2022.
4. Marcus Comiter. Attacking Artificial Intelligence AI's Security Vulnerability and What Policymakers Can Do About It. [Электронный ресурс]. – 2019. – Режим доступа: https://belfercenter.org/sites/default/files/2019-08/AttackingAI/AttackingAI.pdf. Дата доступа: 28.04.2022.
5. Атаки на нейронные сети: как избежать неприятностей? [Электронный ресурс]. – 2020. – Режим доступа: https://smartengines.ru/blog/neural-net-attacks/?ysclid=l14vb30hm2. Дата доступа: 28.04.2022.

ПРИКЛАДНЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ КРИПТОГРАФИЧЕСКОЙ И ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.056.5

МЕТОД ОЦЕНКИ ЗАЩИЩЕННОСТИ РЕЧЕВОГО СИГНАЛА ПО ЕГО ОГИБАЮЩЕЙ

[1]В.К. ЖЕЛЕЗНЯК, Е.Р. [1]АДАМОВСКИЙ, [2]А.Г. ФИЛИППОВИЧ
[1]Полоцкий государственный университет, г. Новополоцк, 211440, Республика Беларусь
[2]Оперативно-аналитический центр при Президенте Республики Беларусь, г. Минск, Республика Беларусь

Введение. Актуальность разработки способов оценки защищенности для каналов утечки информации (КУИ) речевых сигналов обусловлена отсутствием единой однозначной модели восприятия речи [1, 2], что препятствует созданию цельной методики для данной задачи.

Речевой сигнал характеризуется сложным набором частотных составляющих в диапазоне до 10-13 кГц [4], которые, в зависимости от озвучиваемого текста, пола, возраста, эмоционального состояния диктора, а также языка, способны значительно варьировать. При этом, во временной области для речевого сигнала может быть вычислена огибающая, которая отражает медленные изменения его амплитуды. Спектр результирующего сигнала достаточно предсказуем в частотной области, и сосредоточен в узкой полосе от 0 до 20-30 Гц, что открывает возможности для улучшения качества оценки.

Поскольку питание усилителей осуществляется через сеть переменного тока, то изменение потребления тока нагрузки приводит к его нестабильности на входе стабилизатора [3]. Таким способом речевой сигнал из питаемой микрофонной системы способен проникать в электромагнитный КУИ, являясь частью излучения усилителя.

В данной работе предложен метод оценки защищенности КУИ на основе анализа огибающей измерительного речевого сигнала в точке наблюдения и реализована имитационная модель метода.

Математический анализ. Рассмотрим аналитический сигнал $s(t)$, который является комплексной функцией, реальная $s_{re}(t)$ и мнимая $s_{im}(t)$ части которого связаны преобразованием Гильберта [5]. Практическая значимость соотношения (1) заключается в возможности выделения из его частей мгновенной амплитуды $u(t)$, фазы $\varphi(t)$ и частоты $\omega(t)$ исходного сигнала (2-4), что применимо и к реальным сигналам, представленным на практике в виде компонента $s_{re}(t)$.

$$s_{im}(t) = \int_{-\infty}^{\infty} s_{re}(\tau)/\pi(t-\tau)d\tau \quad (1)$$

$$u(t) = \sqrt{s_{re}^2(t) + s_{im}^2(t)} \quad (2)$$

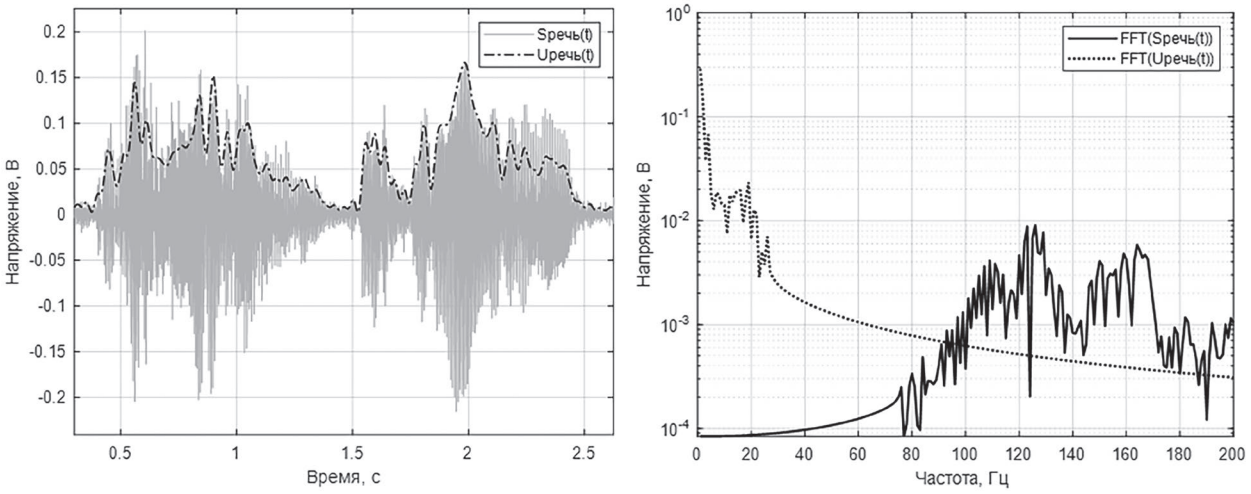
Набор значений мгновенной амплитуды $u(t)$ соответствует понятию огибающей сигнала, которой оперируют при обработке амплитудно-модулированных (АМ) сигналов. Рассмотрим АМ-сигнал $s(t)$, который получен путем перемножения модулируемого $s_c(t)$ и модулирующего $s_e(t)$ сигналов единичной амплитуды [6] с заданным коэффициентом корреляции m (3-4):

$$s(t) = (1 + m \times s_e(t)) \times s_c(t) \quad (3)$$

$$m = s(t)_{макс} - s(t)_{мин} / s(t)_{макс} + s(t)_{мин} \quad (4)$$

В наиболее распространенном на практике случае, когда несущее колебание является гармоническим колебанием, то сигнал $s_e(t)$ соответствует $u(t)$ по частоте и отличается от него в m раз по амплитуде. Для случая, когда модулируется не одна, а множество гармоник (речевой сигнал), форма огибающей приобретает сложную форму, поскольку отражает мгновенные амплитуды интерференции составляющих его частот, а не их сумму [5].

На рис. 1 показан речевой сигнал $s_{речь}(t)$ (запись фразы «добрый день, как вас зовут?» длительностью 3 с), где область частот ниже 75 Гц вырезана с целью устранения помех сети; и выделенная огибающая $u_{речь}(t)$, где частоты выше 30 Гц подавлены. Следует отметить, что в огибающей после фильтрации, соответствующей удалению 99% спектральных отсчетов, остается около 25% ее исходной мощности.



а) б)

Рис.1. Речевой сигнал и его огибающая: а) временная область; б) частотная область

Присутствие амплитудной модуляции в КУИ может быть вызвано процессами, не связанными с работой устройства, для которого осуществляется оценка защищенности. Таким образом, требуется установить взаимосвязь между излучаемым сигналом и сигналом в точке наблюдения. В качестве меры схожести последовательностей используют коэффициент корреляции Пирсона (7), обозначаемый как R [7]:

$$R = \frac{M\left[\left(s(t) - M\left[s(t)\right]\right) \times \left(u(t) - M\left[u(t)\right]\right)\right]}{\sigma_{s(t)} \times \sigma_{u(t)}} \quad (10)$$

где M – математическое ожидание;
σ – стандартное отклонение.

Коэффициент корреляции R отражает то, насколько изменение одной величины влияет на другую, при этом вариация абсолютных амплитуд сигналов не изменяет результат.

Метод оценки защищенности КУИ. Метод оценки заключается в генерации и излучении измерительного сигнала, огибающая которого сравнивается с огибающей колебания в точке наблюдения. Величина, обратная амплитуде корреляции между ними определяет

степень защищенности КУИ. Схема модели представлена на рис. 2. Алгоритм включает следующие шаги:

1. Генерация измерительного АМ-сигнала $s_{тест}(t)$ в речевом диапазоне частот согласно (5-6). При этом модулируемое многочастотное колебание $s_{с.тест}(t)$ должно включать набор кратных гармоник основного тона $f_N = N \times f_1$, который лежит в области 100-150 Гц, а модулирующее колебание $s_{е.тест}(t)$ должно иметь квазипериодическую структуру в области до 30 Гц.
2. Выделение огибающей $u_{тест}(t)$ из измерительного АМ-сигнала (2). В общем случае $u_{тест}(t)$ эквивалентно $s_{е.тест}(t)$, следовательно, шаг является необязательным в случае синтезированного сигнала $s_{тест}(t)$.
3. Излучение измерительного сигнала $s_{тест}(t)$ в КУИ и его измерение в точке наблюдения как $s_{куи}(t)$. В простейшей модели полученный сигнал $s_{тест}(t)$ может быть представлен как аддитивная смесь $s_{тест}(t)$ с шумом КУИ $w(t)$.
4. Выделение из $s_{куи}(t)$ огибающей $u_{куи}(t)$ аналогично п. 2 (2).
5. Обработка $u_{тест}(t)$ и $u_{куи}(t)$ взаимно-корреляционным способом (7).
6. Сравнение полученной величины R с нормативным пороговым значением $R_{порог}$, определяющим максимально допустимое значение схожести огибающих, при котором канал считается защищенным.

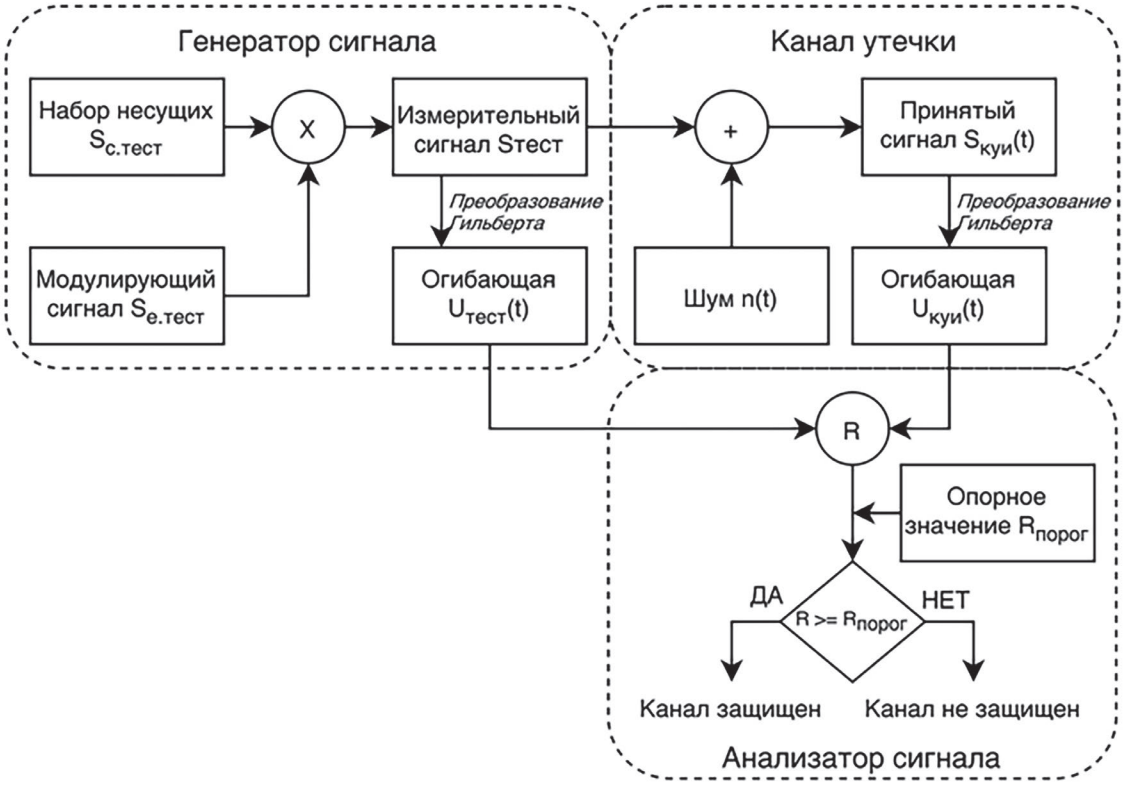


Рис. 2. Алгоритм имитационной модели

Результаты. Имитационная модель реализована с помощью стандартных инструментов программной среды *MatLab*. В качестве шума КУИ использовался аддитивный белый гауссовский шум (*AWGN*). Речевые сигналы были ограничены частотой 48 кГц, разрядность АЦП 16 бит. Коэффициент корреляции R вычислялся с использованием встроенной функции *corrcoef*.

В табл. 1 показаны результаты имитационного моделирования, которые содержат значения коэффициентов взаимной корреляции R и модуляции m измерительных сигналов по итогу 10 измерений, полученные согласно представленному алгоритму.

В качестве измерительных сигналов был использован речевой сигнал $S_{речь}(t)$ – озвученная на русском языке панграмма, выделенная огибающая $U_{речь}(t)$, гармонический АМ-сигнал $S_{гарм.АМ}(t)$ ($m = 1$) и выделенная огибающая $U_{гарм.АМ}(t)$. Исходные речевые сигналы подвергались зашумлению во всей полосе частот с отношением сигнал/шум (ОСШ) по мощности от плюс 15 дБ до минус 25 дБ с шагом 5 дБ. Также представлен случай, когда шум отсутствует.

В результате были получены сигналы $S_{гарм.КУИ}(t)$, $U_{гарм.КУИ}(t)$, $S_{гарм.АМ.КУИ}(t)$ и $U_{гарм.АМ.КУИ}(t)$ соответственно. Огибающие ограничивались по частоте до 30 Гц. Измерено соотношение исходного m и полученного $m_{30.Гц.КУИ}(t)$ коэффициента модуляции для сравнения со значениями корреляции R. Дополнительно для анализа сигналов $U_{речь}(t)$ и $U_{речь.КУИ}(t)$ был реализован вариант без ограничения огибающей по частоте 30 Гц для исследования влияния высокочастотной (ВЧ) составляющей на результаты моделирования, измерено соответствующее значение $m_{КУИ}$.

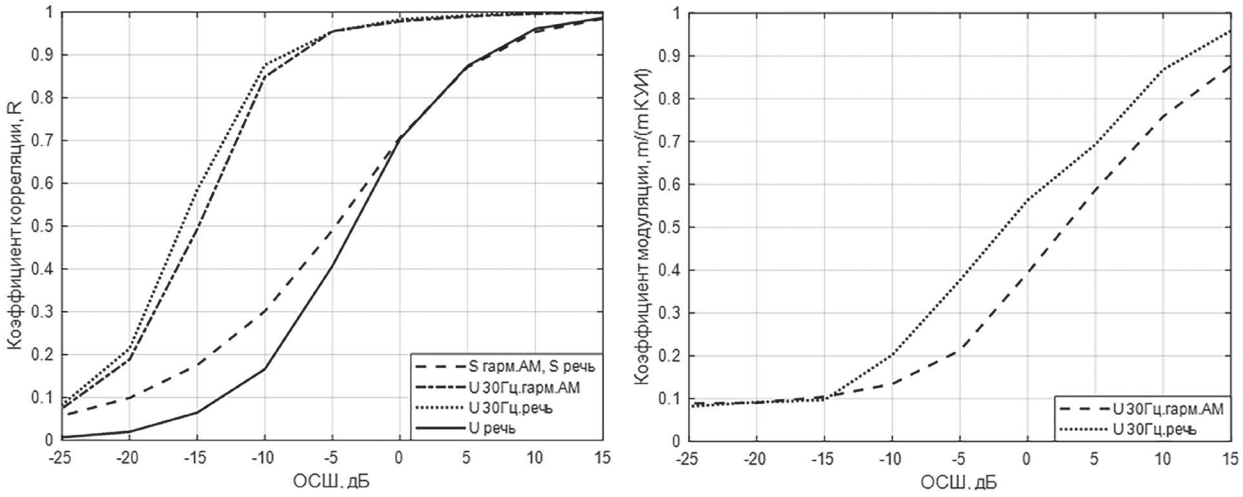
Таблица 1. Коэффициенты корреляции и модуляции сигналов в шумах

ОСШ, дБ	$U_{речь}(t)$ и $U_{речь.КУИ}(t)$				$S_{речь}(t)$ и $S_{речь.КУИ}(t)$	$U_{гарм.АМ}(t)$ и $U_{гарм.АМ.КУИ}(t)$		$S_{гарм.АМ}(t)$ и $S_{гарм.АМ.КУИ}(t)$
	$R_{30.Гц}$	$m_{30.Гц.КУИ}$	R	$m_{КУИ}$	R	$R_{30.Гц}$	$m_{30.Гц.КУИ}$	R
нет	1	1	1	1	1	1	1	1
+15	0.999	0.9586	0.986	0.9998	0.9845	0.9989	0.8760	0.9845
+10	0.997	0.8678	0.960	0.9997	0.9534	0.9963	0.7586	0.9534
+5	0.992	0.6932	0.874	0.9998	0.8715	0.9897	0.5872	0.8715
0	0.982	0.5633	0.703	0.9999	0.7067	0.9782	0.3938	0.7071
-5	0.954	0.3765	0.407	1	0.4902	0.9552	0.2126	0.4903
-10	0.876	0.2020	0.166	0.9985	0.3012	0.8485	0.1342	0.3013
-15	0.584	0.0970	0.064	0.9991	0.1745	0.4929	0.1041	0.1753
-20	0.214	0.0915	0.019	0.9995	0.0994	0.1886	0.0906	0.0988
-25	0.082	0.0817	0.006	0.9992	0.0559	0.0739	0.0884	0.0571

На рис. 3а показаны значения R и $R_{30.Гц}$ согласно табл. 1. Ее анализ показывает, что уровни корреляции между исходным и зашумленным колебанием для речевого и гармонического сигналов практически идентичны, поэтому на рис. 3а они объединены.

На рис. 3б показаны значения $m_{КУИ}$ и $m_{30.Гц.КУИ}$ согласно табл. 1. Не показано значение $m_{КУИ}$ для неограниченной по частоте огибающей речевого сигнала, поскольку из-за влияния шума оно оставалось приблизительно равным единице. Это подтверждает необходимость ограничения огибающей для последующего анализа.

Из рис. 3а следует, что оценка корреляционных свойств сигналов во всей доступной частотной полосе дает низкие значения, поскольку в таком случае влияние широкополосного шума значительно снижает величину меры схожести. Это подтверждается быстрым спадом кривых $S_{гарм.АМ}$ и $S_{речь}$ сигналов, не ограниченных по частоте. Для кривых $U_{речь}$ и $U_{30гарм.АМ}$, соответствующих узкополосным сигналам, убывание $R_{30.Гц}$ с увеличением мощности шума происходит более медленно, особенно для огибающей речевого сигнала.



а) б)

Рисунок 3. Результаты имитационного моделирования, сравнение: а) коэффициента взаимной корреляции; б) коэффициента модуляции

Рис. 3б демонстрирует характер падения коэффициента модуляции $m_{30.Гц.КУИ}$, вычисленного по огибающим сигналов. Показано, что модуляция речевого сигнала более устойчива к шуму, чем гармонического модулированного сигнала. Преимущество сохраняется до уровня помех -15 дБ, а затем в обоих случаях $m_{30.Гц.КУИ}$ выходит на плато значений 0.09-0.1, соответствующее фоновому уровню m практически случайных колебаний.

Заключение. Представлен метод оценки защищенности канала утечки информации на основе взаимно-корреляционного анализа огибающей измерительного сигнала в речевом диапазоне частот и результаты имитационного моделирования метода. Произведен сравнительный анализ результатов для огибающей речевого сигнала, исходного речевого сигнала и гармонического амплитудно-модулированного сигнала. Показаны преимущества использования огибающей речевого сигнала для оценки защищенности канала утечки информации.

Список литературы

1. Анохин В.В., Герасименко Е.А., Кондратьев А.В. Рассмотрение критериев защищённости речи на основе словесной и смысловой разборчивости // Специальная техника. 2016. № 6. С. 22-28.
2. Шелухин О.И. Цифровая обработка и передача речи. М.: Радио и связь, 2000. 456 с.
3. Костиков В.Г., Парфенов Е.М., Шахнов В.А. Источники электропитания электронных средств. Схемотехника и конструирование. М.: Горячая линия–Телеком, 2001. 344 с.
4. Трушин В.А., Иванов А.В., Рева И.Л. О корректировке методики оценки защищённости речевой информации от утечки по техническим каналам // Специальная техника. 2016. № 6. С. 22-30.
5. Бутырский Е.Ю. Преобразование гильберта и его обобщение // Научное приборостроение. 2014. № 24(4). С. 30-37.
6. Баскаков С.И. Радиотехнические цепи и сигналы. М.: Ленанд. 2016; 528.
7. Рябенко Д.С., Лавров С.В., Боровкова Е.С. Приложение сигнальных графов и матричного анализа для математического моделирования каналов утечки информации // Вестник Полоцкого государственного университета. Серия С. Фундаментальные науки. 2018 № 4. С. 56-60.

УДК 621.391.16; 681. 327.8

ДОСТОВЕРНЫЙ КОНТРОЛЬ ЗАЩИЩЕННОСТИ КВАНТОВАННОГО И ВОССТАНОВЛЕННОГО РЕЧЕВОГО СИГНАЛА

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

Введение

Повсеместное использование современных цифровых технологий неразрывно связанно с применением аналого-цифровых и цифро-аналоговых преобразователей. Установлено, что преобразование аналоговых речевых сигналов в цифровые и их обратное преобразование из цифровой формы в исходный сигнал генерируют новые каналы утечки речевой информации [1].

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

Кроме того, 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 [1].

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

1. Особенности дискретно-квантованного преобразования речевых сигналов

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

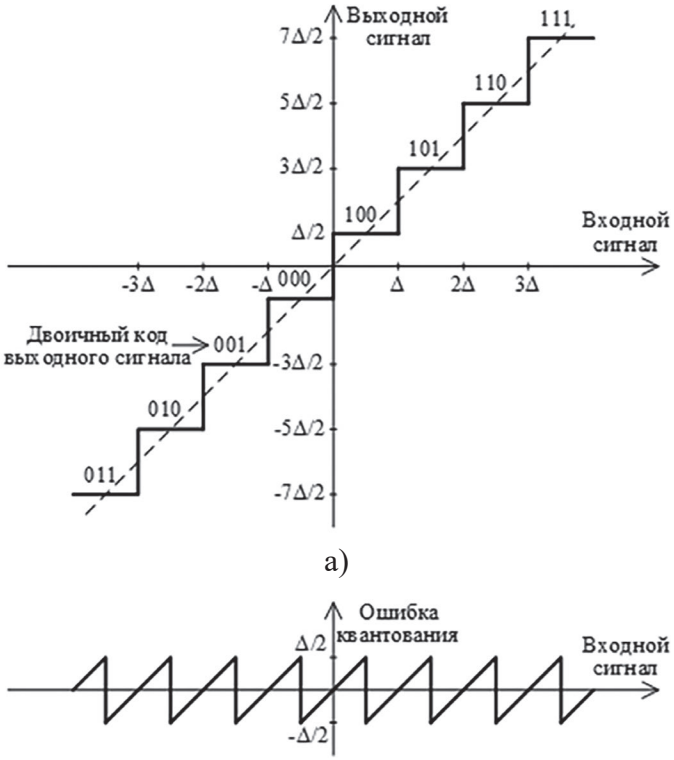
При равномерном квантовании с числом уровней квантования $L = 2^N$ (где N – число бит цифровой передачи) величину шага квантования Δ определяют по формуле:

$$\Delta = \frac{U_{\max}}{2^N}, \qquad (1)$$

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

На рисунке 1 (а) приведена амплитудная характеристика квантования.

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



а)

б)

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

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

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

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

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

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

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

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

$$SNR = 6,02N + 10\lg\left(\frac{F_д}{2\Delta f_B}\right) + C_s, \tag{5}$$

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

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

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

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

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

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

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

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

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

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

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

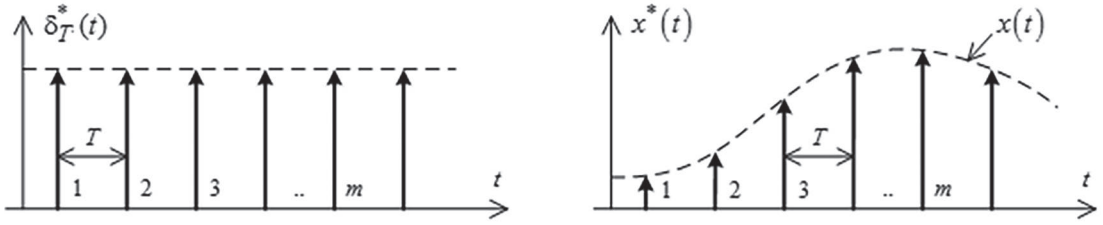


Рисунок 2. Модулированная последовательность δ-функций

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

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

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

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

- высокой погрешность оценки отношения уровня дискретизированного речевого сигнала к уровню шума квантования из-за того, что и сигнал, и шум квантования – случайные процессы;
- низкой точность и достоверность оценки защищенности, обусловленной искажением сигнала шума квантования из-за высокого по сравнению с его уровнем шума в точке наблюдения;
- отсутствием нормативного значения оценки защищенности речевого сигнала, преобразованного квантованно-дискретным преобразованием для передачи в широкополосных каналах.

2. Оценка защищенности дискретно-квантованного речевого сигнала

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

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

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

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

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

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

где k = 1, 2, 3, …

Для формирования измерительного сигнала, в качестве исходного (нормированного) сигнала используем периодическую импульсную последовательность прямоугольной формы с периодом Т, 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.

Преобразуем автокорреляционной функцией периодическую импульсную последовательность прямоугольной формы в периодическую импульсную последовательность треугольной формы. В результате преобразования получим необходимый измерительный сигнал, представленный в виде периодической импульсной последовательности треугольной

формы с мощностью $A^2\tau$ и длительностью импульса 2τ [1], где A – амплитуда импульса импульсной последовательности прямоугольной формы и τ = 1000; 769; 625; 526; 444; 385; 333; 294; 267; 243; 222; 206; 183; 161; 143; 130; 110; 81; 58 мкс (рисунок 3).

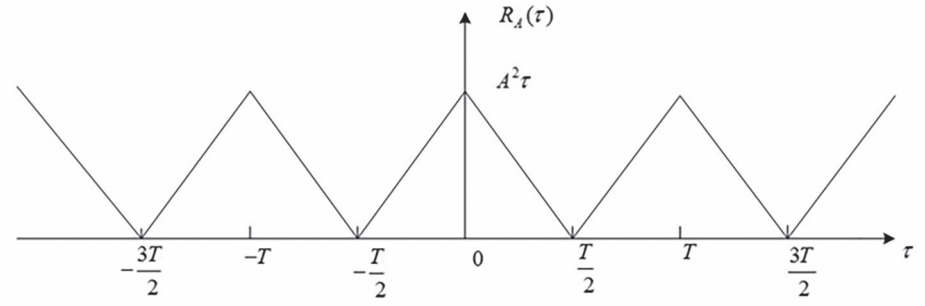


Рисунок 3. Автокорреляционная функция

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

Заключение

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

Список литературы

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. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. – Москва: Горячая линия – Телеком, 2017. – 586 с.
3. Железняк, В.К. Защита информации от утечки по техническим каналам : учеб. пособие / В.К. Железняк. – Санкт-Петербург: ГУАП, 2006. – 188 с.
4. Шкритек, П. Справочное руководство по звуковой схемотехнике / П. Шкритек. – Москва: Мир, 1991 – 446 с.
5. Цыпкин, Я.З. Основы теории автоматических систем / Я.З. Цыпкин. – Москва: Наука, 1977. – 560 с.
6. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – Москва: Вильямс, 2007. – 1104 с.

УДК 004.056.55

О РОССИЙСКИХ СТАНДАРТИЗИРОВАННЫХ РЕШЕНИЯХ В ОБЛАСТИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ И ПЕРСПЕКТИВАХ ИХ ИСПОЛЬЗОВАНИЯ В РАМКАХ СОЮЗНОГО ГОСУДАРСТВА

А.И. БОНДАРЕНКО
Академия криптографии Российской Федерации
Москва, *119331,* Российская Федерация

Информационные технологии определяют процессы, методы поиска, сбора, хранения, обработки, предоставления и распространения информации. Одной из проблем при внедрении информационных технологий в масштабе любого государства является различие способов обработки информации и ее защиты. Унификация таких способов на основе документов нормативно-технического регулирования – стандартов в области информационных технологий, обеспечивающих возможность использования единых сквозных подходов, является одним из способов решения указанной проблемы. Неотъемлемой частью любой системы стандартов в области информационных технологий являются стандарты в области криптографии и безопасности информационных технологий, реализация которых является необходимым условием для обеспечения надежного и безопасного функционирования информационных технологий, а в некоторых случаях и «знаком качества», определяющим уровень доверия. В настоящем докладе рассмотрим, как за прошедшие годы изменялись криптографические стандарты Российской Федерации, а также постараемся выделить актуальные направления развития информационных технологий Союзного государства, технологии криптографической защиты которых могут базироваться на соответствующих межгосударственных стандартах и реализовываться в соответствии с ними.

В 80-х годах прошлого века был проведен цикл фундаментальных поисковых исследований по теме «Магма», длившихся не один год, в результате которых был разработан блочный шифр, и Постановлением Государственного комитета СССР по стандартам от 2 июня 1989 года № 1409 был утвержден и введен в действие – ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» [1]. Разработанный стандарт включал описание блочного шифра с длиной входного

блока 64 бита и длиной ключа 256 битов, а также ряда режимов его работы, предназначенных для обеспечения конфиденциальности и контроля целостности данных.

В начале 90-х годов двадцатого века произошли существенные изменения в сфере экономики, синхронизировавшиеся по времени с всеобщим развитием информационных технологий и телекоммуникационных сетей связи. Именно эти факторы потребовали разработки механизмов контроля целостности и подтверждения авторства передаваемой по каналам связи информации, которые должны были обеспечить базовые механизмы аутентификации пользователей и серверов в многопользовательских недоверенных сетях связи, например, в сети Интернет. Эти криптографические механизмы были реализованы в новых, для того момента времени, стандартах:

- ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе ассиметричных криптографических алгоритмов» [2];
- ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования» [3].

Описанная в ГОСТ Р 34.10-94 схема электронной цифровой подписи (далее – ЭЦП) была основана на одном из вариантов широко известной обобщенной схемы Эль-Гамаля с порядком подгруппы 256 бит. Хэш-функция, описанная в стандарте ГОСТ Р 34.11-94, основана на композиции нескольких реализаций блочного шифра, определенного ГОСТ 28147-89, и имела длину хэш-кода, равную 256 битов.

До начала 2000-х годов указанные три стандарта первого поколения служили технологической основой криптографических механизмов защиты. Они были приняты Межгосударственным советом по стандартизации, метрологии и сертификации на территории Содружества Независимых Государств (далее – МГС) в качестве одноименных межгосударственных стандартов — ГОСТ 28147-89 [1], ГОСТ 34.310-95 [4] и ГОСТ 34.311-95 [5] соответственно.

В течение последующих нескольких лет получил существенное развитие математический аппарат и методы анализа схем ЭЦП. Это привело к тому, что в новом веке были достигнуты определенные успехи в решении задачи логарифмирования в конечном простом поле. Данное обстоятельство потребовало осуществить переход к схеме ЭЦП, стойкость которой основывается на предположении о вычислительной трудности решения задачи дискретного логарифмирования в группе точек эллиптической кривой. В 2001 году был принят национальный стандарт ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», призванный заменить ГОСТ Р 34.10-94.

Криптографические преобразования в новой схеме электронной подписи, определенной ГОСТ Р 34.10-2001 [6], позволили существенно повысить уровень криптографической стойкости и быстродействия схемы ЭЦП по сравнению со схемой ЭЦП, реализующей преобразования в конечном простом поле, за счет использования более компактной алгебраической структуры. В 2004 году был обновлен и введен в действие соответствующий межгосударственный стандарт ЭЦП – ГОСТ 34.310-2004 [7].

В это же время представителями российских предприятий была начата работа над расширением списка криптографических механизмов, использующих российские криптографические алгоритмы, определенные в национальных стандартах. Так, в первой половине 2000-х годов на площадке Инженерного совета Интернета — IETF были разработаны сле-

дующие стандарты сети Интернет (RFC), содержащих описание российских механизмов криптографической защиты информации:

- RFC 4357 «Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001 and GOST R 34.11-94 Algorithms» [8];
- RFC 4490 «Using the GOST 28147-89, GOST R 34.10-94, GOST R 34.11-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)» [9],
- RFC 4491 Using the GOST 28147-89, GOST R 34.10-94, GOST R 34.11-94, and GOST R 34.10-2001 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile» [10],
- RFC 5830 «GOST 28147-89: Encryption, Decryption and Message Authentication Code (MAC) Algorithms» [11],
- RFC 5831 «GOST R 34.11-94: Hash Function Algorithm» [12],
- RFC 5832 « GOST R 34.10-2001: Digital Signature Algorithm» [13].

Однако необходимость более тесного взаимодействия разработчиков средств криптографической защиты информации, интеграторов и научного сообщества при разработке спецификаций криптографических механизмов потребовала создания отдельной площадки. Так в 2007 году под эгидой Федерального агентства по техническому регулированию и метрологии (Росстандарт) был создан Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26).

Первым результатом планомерной и продолжительной работы российских экспертов ТК 26 в профильной рабочей группе Международной организации по стандартизации (2 рабочая группа 27 подкомитета 1-го объединенного комитета Международной организации по стандартизации/Международной электротехнической комиссии (ИСО/МЭК)) стало включение в 2010 году схемы ЭЦП, описанной в ГОСТ Р 34.10-2001, в международный стандарт ISO/IEC 14888-3 «Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms» [14]. Данный международный стандарт включает в себя описание двенадцати схем ЭЦП (американский, корейский, немецкий вариант и т.д.), среди которых одна схема на протяжении последних 12 лет является российской схемой ЭЦП.

Первое десятилетие XXI века ознаменовалось бурным развитием методов криптографического анализа функций хэширования: многие существовавшие на тот момент криптографические решения, например, SHA-1 (стандарт США на тот момент) или MD5, были теоретически «сломаны», что в дальнейшем привело к возможности построения практически реализуемых атак. Не избежала «попыток» криптоанализа и функция хэширования ГОСТ 34.11-94 [3]. Хотя предложенная атака была исключительно теоретической и до сегодняшнего дня не привела к возникновению реальных уязвимостей, появилась необходимость ее обновления. Кроме этого, практические приложения потребовали определения спецификаций для более длинной 512 битной ЭЦП. В результате в 2012 году были утверждены стандарты:

- ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» [15];
- ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» [16].

Данные стандарты включают теперь два варианта криптографических механизмов (256битные и 512-битные) – схемы ЭЦП и кардинальной новой функции хэширования, по-

лучившей название «Стрибог». Также они вывели из действия одноименные ГОСТ Р 34.10-2001 [6] и ГОСТ Р 34.11-94 [3].

При резко возросших объемах передаваемой информации наибольшие проблемы представляла собой именно короткая 64-битная длина входного блока ГОСТ 28147-89 [1]. Именно это обстоятельство в наибольшей степени послужило причиной разработки нового блочного шифра «Кузнечик», который в 2015 году был включен в ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры» [17]. Данный стандарт также включает блочный шифр из ГОСТ 28147-89 [1] с фиксированными долговременными параметрами под новым названием «Магма». Режимы работы блочных шифров были теперь определены отдельным стандартом ГОСТ Р 34.13-2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров» [18] и концептуально увязаны с режимами работы блочных шифров, определяемыми широко используемыми международными стандартами ISO/IEC 10116 «Information technology – Security techniques – Modes of operation for an n-bit block cipher» [19] и ISO/IEC 9797-1 «Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher» [20].

Впоследствии, в 2018 года все четыре базовых российских криптографических стандарта были приняты МГС в качестве межгосударственных стандартов – ГОСТ 34.10-2018 [21], ГОСТ 34.11-2018 [22], ГОСТ 34.12-2018 [23], ГОСТ 34.13-2018 [24]. Здесь стоит высказать слова благодарности нашим партнерам, которые поддержали принятие указанных стандартов в МГС.

Дополнительно, хотелось бы отметить большую работу российских специалистов в части подготовки стандартов сети Интернет (RFC), благодаря которым все действующие российские стандарты в области криптографической защиты информации определены в:

- RFC 6986 «GOST R 34.11-2012: Hash Function» [25];
- RFC 7091 «GOST R 34.10-2012: Digital Signature Algorithm» [26];
- RFC 7801 «GOST R 34.12-2015: Block Cipher “Kuznyechik”»[27];
- RFC 8891 «GOST R 34.12-2015: Block Cipher “Magma”» [28].

Одновременно с этим следует отметить, что российские эксперты в Международной организации по стандартизации добились включения функции хэширования «Стрибог» в новую редакцию международного стандарта ISO/IEC 10118-3 «Information technology – Security techniques – Hash functions – Part 3: Dedicated hash-functions» [29], опубликованную в октябре 2018 года.

Начиная с 2015 года экспертами ТК 26 был проведен значительный объем работ по расширению номенклатуры документов национальной системы стандартизации в области криптографической защиты информации и их ориентирование в отраслевом направлении. Начиная с 2016 года по настоящее время разработано и утверждено 36 рекомендации по стандартизации Росстандарта (далее – рекомендации). В 2022 году в плановой разработке (в разной степени готовности) находятся 11 проектов рекомендации по стандартизации и 29 проектов методических рекомендаций. Детальный рассказ о каждом документе по стандартизации занял бы значительной период время, в этой связи рассмотрим наиболее основные из них.

1. Документы по стандартизации общего назначения, которые не определяют или не подразумевают использование описываемого криптографического механизмам или решения для определенной функциональной области или отрасли. Среди таких ме-

ханизмов, можно выделить следующие криптографические механизмы или решения, описанные в рекомендациях:

- варианты криптографических функций выработки производного ключа, описанные в рекомендациях Р 1323565.1.017-2018 и Р 1323565.1.0222018;
- варианты криптографических функций выработки псевдослучайных последовательностей, описанные в рекомендациях Р 1323565.1.006-2017;
- схема выработки общего ключа с аутентификацией на основе открытого ключа и на основе пароля соответственно, описанные в рекомендациях Р 1323565.1.004-2017 и Р 50.1.115-2016;
- режим имитозащищенного шифрования MGM, т.е. режима шифрования обеспечивающий одновременно конфиденциальность и имитозащиту данных, описанный в рекомендациях Р 1323565.1.026-2019;
- варианты представления эллиптических кривых в форме Эдвардса, описанные в рекомендациях Р 50.1.114-2016;
- границы на допустимый объём материала, обрабатываемый на одном ключе, для стандартизированных режимов работы блочных шифров, описанные в рекомендациях Р 1323565.1.005-2017;
- принципы разработки и модернизации шифровальных средств, описанные в рекомендациях Р 1323565.1.012-2017, в которых определяются вопросы безопасности практических реализаций средств криптографической защиты информации

Без подобных сопутствующих криптографических механизмов нельзя представить функционирование современных криптографических решений, телекоммуникационных протоколов и иных криптографических механизмов, реализуемых в актуальных средствах криптографической защиты информации. Например, значительная часть описанных выше криптографических механизмов используется при описании российских вариантов протоколов TLS 1.2 и 1.3.

2. Отраслевые документы по стандартизации, которые описывают криптографические механизмы или решения, подразумевающие использование в определенной функциональной области или отрасли. Можно выделить следующие отраслевые направления использования российских криптографических решений:

2.1. Системы электронного документооборота, к криптографическим решениям в которой можно отнести следующие:

- контейнер хранения ключей и транспортный ключевой контейнер, описанные в рекомендациях Р 50.1.110–2016 и Р 50.1.112–2016 соответственно (в настоящее время осуществляется их плановый пересмотр);
- порядок использования российских криптографических алгоритмов в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509, описанный в рекомендациях Р 1323565.1.023-2022;
- форматы сообщений (CMS), защищенных криптографическими методами, описанные в рекомендациях Р 1323565.1.025-2019;
- использование российских алгоритмов электронной подписи в протоколах и форматах сообщений на основе XML, описанное в рекомендациях Р 1323565.1.033-2020;

- использование российских криптографических алгоритмов в протоколе штампов времени (TSP), описанное в методических рекомендациях МР 26.2.001 – 2021, и т.д.

Разработанные криптографические решения способствуют встречной и безопасной работе средств криптографической защиты информации, используемых в системах защищенного электронного документооборота, а также способствуют блокированию атак высококвалифицированного нарушителя на указанные системы.

2.2. Национальные системы платежных карт, к криптографическим решениям в которой можно отнести:

- использование российских криптографических алгоритмов при формировании проверочного параметра платежной карты и проверочного значения PIN, описанное в рекомендациях Р 1323565.1.007-2017;
- использование российских криптографических алгоритмов в защищенном обмене сообщениями между эмитентом и платежным приложением, описанное в рекомендациях Р 1323565.1.008-2017;
- задание параметров российских криптографических алгоритмов в профиле EMV сертификатов открытых ключей платёжных систем, описанное в рекомендациях Р 1323565.1.015-2018, и т.д.

Разработанные рекомендации полностью определяют место и возможность использования российских криптографических алгоритмов в составе технологий, описанных в стандарте EMV, а также условия их применения в национальных системах платежных карт, в том числе платежной системе «МИР» и соответствующей платежной инфраструктуре – POS, ATM, банковское ПО, УЦ и т.д. Применение указанных рекомендаций является достаточным для реализации в любой системе платежных карт стандартного набора сервисов с использованием российских криптографических алгоритмов.

2.3. Современные телекоммуникационные сети, в том числе сеть Интернет, к криптографическим решениям в которой можно отнести:

- использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2), описанное в рекомендациях Р 1323565.1.020-2020;
- использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3) и контрольные примеры к ним, описанные в рекомендациях Р 1323565.1.030-2020 и в методических рекомендациях МР 26.2.002 – 2021;
- использование российских криптографических алгоритмов в протоколе защиты информации (ESP), описанное в рекомендациях Р 1323565.1.035-2021;
- использование российских криптографических алгоритмов в протоколе обмена ключами в сети Интернет версии 2 (IKEv2), описанное в методических рекомендациях МР 26.2.001 – 2022;
- протокол безопасности сетевого уровня (IPlir), описанный в рекомендациях Р 1323565.1.034-2020, и т.д.

Использование данных протокольных решений при доступе к информационным ресурсам сети Интернет (в том числе к сайтам органов государственной власти и организаций) позволяет существенно повысить уровень криптографической

защиты телекоммуникационного соединения пользователя и сервера, реализуя независимую от иностранных элементов цепочку доверия.

Следует отметить, что в 2019 году организация IANA (Internet Assigned Numbers Authority), управляющая идентификаторами и параметрами протоколов сети Интернет, одобрила по результатам экспертизы включение идентификаторов российских криптографических алгоритмов в реестр идентификаторов для протокола TLS 1.2. В 2022 году согласно RFC 9189 «GOST Cipher Suites for Transport Layer Security (TLS) Protocol Version 1.2» [30] данные идентификаторы были полноправно включены в указанный реестр. В настоящее время проект по внесению идентификаторов российских криптографических алгоритмов в реестр идентификаторов IANA для протокола TLS 1.3 находится на завершающей стадии рассмотрения.

В 2022 году согласно RFC 9227 «Using GOST Ciphers in the Encapsulating Security Payload (ESP) and Internet Key Exchange Version 2 (IKEv2) Protocols» [31] идентификаторы российских криптографических алгоритмов были включены в реестр идентификаторов IANA для протоколов ESP и IKEv2.

2.4. Интернета вещей, к криптографическим решениям в котором можно отнести:

- криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств, описанное в рекомендациях Р 1323565.1.028-2019;
- использование российских криптографических механизмов для реализации обмена данными по протоколу DLMS, описанное в рекомендациях Р 1323565.1.032-2020;
- протокол защищенного обмена для индустриальных систем (CRISP), описанный в рекомендациях Р 1323565.1.029-2019, и т.д.

Описанные криптографические решения используются преимущественно в гражданском секторе применения криптографии, связанном с гарантированным и защищенным криптографическими методами контролем и распределением энергетических, газовых, нефтяных, водных и иных ресурсов.

2.5. Контрольно-кассовая техника, к криптографическим решениям в которой можно отнести:

- криптографические механизмы аутентификации и выработки ключа фискального признака для применения в средствах формирования и проверки фискальных признаков, обеспечивающих работу контрольно-кассовой техники, операторов и уполномоченных органов обработки фискальных данных, описанные в рекомендациях Р 1323565.1.019-2018, и т.д.

Реализация в контрольно-кассовой технике указанных криптографических решений позволяет существенно сократить возможность нарушителя по совершению мошеннических и иных противоправных действий, связанных с налоговыми махинациями.

2.6. Мобильная связь третьего и последующих поколений, к криптографическим решениям в которой можно отнести:

- криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов, предназначенные для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи, описанные в рекомендациях Р 1323565.1.003-2017, и т.д.

Использование данных криптографических алгоритмов позволяет в первую очередь с использованием доверенных российских криптографических решений обеспечить конфиденциальность и контроль целостности голосового трафика и иной информации, циркулирующей в сетях сотовой связи третьего и последующих поколений, в том числе реализуя независимую от иностранных технологий процедуру создания ключей.

2.7. Контрольные устройства для автотранспорта, к криптографическим решениям в которых можно отнести:

- криптографические механизмы аутентификации в контрольных устройствах для автотранспорта, описанный в рекомендациях Р 1323565.1.018-2018, и т.д.

3. Новые направления в области криптографической защиты информации.

3.1. Квантовые системы связи, к криптографическим решениям в которых можно отнести:

- защищенный протокол взаимодействия квантово-криптографической аппаратуры выработки и распределения ключей и средства криптографической защиты информации, описанный в методических рекомендациях МР 26.4.004 – 2021;
- ключевые системы сетей шифрованной связи с использованием квантовой криптографической сети, которые будут описаны в разрабатываемых в настоящее время методических рекомендациях;

3.2. Постквантовые криптографические алгоритмы:

- постквантовая схема электронной подписи, построенной на основе кодов, исправляющих ошибки, которая будет описана в разрабатываемых методических рекомендациях;
- постквантовая схема инкапсуляции ключа, построенная на основе изогений эллиптических кривых, которая будет описана в разрабатываемых методических рекомендациях;
- постквантовые криптографические механизмы, построенные на основе хэш-функций, которые будут описаны в разрабатываемых методических рекомендациях;
- постквантовая схема электронной подписи, построенной на решеток, которая будет описана в разрабатываемых методических рекомендациях, и т.д.;

Криптографические решения из данной группы в первую очередь направлены на создание научного задела в фундаментальных областях криптографии, введение которых в перспективе может оказаться востребованным.

Благодаря активной позиции российских экспертов в Инженерном совете Интернета (IETF) многие из описанных выше и стандартизированных в Российской Федерации криптографических механизмов к настоящему моменту описаны в международных рекомендациях RFC, а именно:

- RFC 7836 «Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.10-2012» (Р 50.1.113-2016) [32];
- RFC 8133 «The Security Evaluated Standardized Password-Autenticated Key Exchange (SESPAKE) Protocol» (Р 50.1.115-2016) [33];
- RFC 8645 «Re-keying Mechanisms for Symmetric Keys» (Р 1323565.1.017-2018) [34];
- RFC 9058 «Multilinear Galois Mode (MGM)» (Р 1323565.1.026-2019) [35];
- RFC 9189 «GOST Cipher Suites for Transport Layer Security (TLS) Protocol Version 1.2» (Р 1323565.1.020-2020) [30];

- RFC 9215 «Using GOST R 34.10-2012 and GOST R 34.11-2012 Algorithms with the Internet X.509 Public Key Infrastructure» (P 1323565.1.023-2022) [36];
- RFC 9227 «Using GOST Ciphers in the Encapsulating Security Payload (ESP) and Internet Key Exchange Version 2 (IKEv2) Protocols» (P 1323565.1.035-2021) [31].

Большинство из описанных стандартизированных криптографических решений в Российской Федерации создают необходимую технологическую основу для создания и развертывания доверенного информационного пространства и защищенных сетей связи. Также указанные криптографические решения могут задавать технологическую основу защиты информации для информационных систем и телекоммуникационных сетей, создаваемых и разворачиваемых в интересах Союзного государства, что будет позитивно способствовать реализации Основных направлений реализации положений Договора о создании Союзного государства и соответственно встречным интеграционным процессам Союзного государства. Такая технологическая основа может быть реализована через дальнейшее развитие межгосударственной системы стандартизации в области криптографической защиты информации, то есть придание криптографическим механизмам, стандартизированным на национальном уровне, статуса межгосударственного стандарта в рамках сотрудничества в МГС стран, входящих в состав Союзного государства и Евразийского экономического союза (далее – ЕАЭС). Важно отметить, что межгосударственная стандартизация может реализовываться на паритетных началах через придание соответствующего статуса как российским, так и белорусским криптографическим механизмам, аналогично практикам, принятым в Международной организации по стандартизации – ISO.

Основные направления создания Союзного государства на 2021 – 2023 годы утверждены Декретом Высшего Государственного Совета Союзного государства от 4 ноября 2021 г. № 6 «Об Основных направлениях реализации положений Договора о создании Союзного государства на 2021 – 2023 годы» [37]. В результате анализа указанных Основных направлений можно выделить следующие наиболее перспективные направления, связанные с созданием совместных информационных систем Союзного государства, обязательно требующих обеспечения их криптографической защиты, или гармонизацией требований в области информационной безопасности.

1. Пункт 2.1 Основных направлений определяет утверждение Союзной программы интеграции информационных систем маркировки товаров[1], в соответствии с пунктом 1.4 которой предписывается установление единых способов криптографической защиты средств их идентификации, согласованных и утвержденных в рамках Евразийского экономического союза. В настоящий момент времени данные единые подходы к криптографической защите информации средств идентификации должны базироваться на единых асимметричных криптографических алгоритмах на базе межгосударственного стандарта ГОСТ 34.10-2018 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» [21]. Данное направление является позитивным примером создания совместных защищенных информационных систем Союзного государства, криптографическая защита которых базируется на межгосударственном стандарте в области криптографической защиты информации.

[1] Термины используются в значениях, определенных в Соглашении о маркировке товаров средствами идентификации в Евразийском экономическом союзе от 2 февраля 2018 г. и Решениях Совета Евразийской экономической комиссии, принятых в соответствии с указанным Соглашением.

2. Пункт 1.5 Основных направлений определяет утверждение Союзной программы по гармонизации требований в области обеспечения информационной безопасности в финансовой сфере (в части компетенции Банка России и Национального банка Республики Беларусь), в соответствии с пунктом 3 которой предписывается формирование и актуализация единого набора стандартов, методик и критериев оценки реализации процессов обеспечения информационной безопасности в финансовой сфере. В качестве технологического базиса для группы стандартов, определяющих реализацию процессов обеспечения криптографической защиты информации в финансовой сфере, могли бы рассматриваться документы по стандартизации в области криптографической защиты информации, в том числе, связанные с функционированием национальных систем платежных карт, описанные выше.
3. Пункт 1.8 Основных направлений определяет утверждение Союзной программы по интеграции платежных систем в области национальных систем платежных карт, систем передачи финансовых сообщений и расчетов, системы быстрых платежей …, в соответствии с пунктом 2.1 которой определяется необходимость разработка основных принципов и параметров взаимодействия системы быстрых платежей Банка России (СБП) с системой мгновенных платежей Национального банка Республики Беларусь (СМП) для совершения трансграничных переводов денежных средств, в том числе требований по информационной безопасности. В качестве технологического базиса для таких требований, в части их криптографической защиты, могли бы рассматриваться документы по стандартизации в области криптографической защиты информации, например, описанные выше.
4. Пункт 3.2 Основных направлений определяет утверждение Союзной программы по интеграции информационных систем государственных контролирующих органов по прослеживаемости товаров, в соответствии с пунктом 3.2 которой определяется необходимость определения технической модели взаимодействия между операторами национальных систем прослеживаемости, в том числе определение средств технической и криптографической защиты информации, используемых при информационном обмене между операторами. В качестве одного из требований к таким средствам криптографической защиты информации могут выступать требования о необходимости реализации исключительно криптографических алгоритмов, определяемых в межгосударственных стандартах в области криптографической защиты информации.

Вместе с тем, с учетом наличия технологического задела в области криптографической защиты информации, описанного выше, и возможности их межгосударственной стандартизации в перспективную повестку основных направлений создания Союзного государства на последующие годы могут быть включены следующие высокотехнологичные направления создания информационных систем и телекоммуникационных сетей Союзного государства:

- развертывание инфраструктуры платежных карт Союзного государства. В 2017 годы рядом российских банков были проведены работы по тестированию аппаратных модулей безопасности информационной инфраструктуры платежной системы (HSM) российского производства, реализующих стандартизированные выше криптографические решения. Результаты этого тестирования подтвердили высокие эксплуатационные и защитные свойства указанных HSM и реализуемых в них криптографических решений. Более того, в 2020 году Центральным Банком Российской Федерации введено «Положение о требованиях к обеспечению защиты информации при осуществлении перевода денежных средств и о порядке осуществления Банком России контроля

за соблюдением требований к обеспечению защиты информации при осуществлении денежных средств» от 4 июня 2020 года № 719-П [8], в соответствии с пунктом 5.5 которого операторам значимой платежной системы в соответствии с правилами платежной системы должно обеспечиваться использование с 1 января 2031 года аппаратных модулей безопасности информационной инфраструктуры платежной системы и средств криптографической защиты информации, реализующие криптографические алгоритмы, определенные национальными стандартами Российской Федерации;

- создание информационной инфраструктуры, обеспечивающей реализацию защищенных технологий доступа к информационным ресурсам Союзного государства, расположенных в сети Интернет. В течение последних двух лет в Российской Федерации идет создание Национального удостоверяющего центра, который будет обеспечивать выпуск TLS-сертификатов с применением российских криптографических алгоритмов. На некоторых информационных ресурсах Российской Федерации такие российские сертификаты уже установлены и доступны для использования. Они способны обеспечить аутентификацию сайта и дальнейшее защищенное соединение с использованием российских криптографических алгоритмов и механизмов. Примерами таких российских ресурсов являются – www.gosuslugi.ru, а также сайт Академии криптографии Российской Федерации – www.cryptoacademy.gov.ru, и т.д.;
- создание защищенных систем учета ресурсов на базе технологий Интернета вещей. Постановлением Правительства Российской Федерации от 19 июня 2020 г. № 890 были утверждены «Правила предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности)» [39], которыми предписывается владельцам интеллектуальной системы учета использовать сертифицированные средства криптографической защиты информации, реализующие криптографические алгоритмы, определенные в документах национальной системы стандартизации Российской Федерации. В ближайшее время запланировано проведение соответствующих пилотных проектов;
- создание защищенных сетей сотовой связи третьего и последующих поколений Союзного государства. Начиная с 2018 года в Российской Федерации принимается ряд нормативных актов профильных министерств Российской Федерации, новеллы которых направлены на установления обязательности реализации и использования в HSM и USIM процедур аутентификации и выработки сессионных ключей защиты конфиденциальности и контроля целостности в соответствии с документами национальной системы стандартизации Российской Федерации. Более того, начиная с 2021 года проводится пилотный проект оператором сотовой связи «Воентелеком» по тестированию «нескольких сот сим-карт и аппаратного модуля безопасности (HSM) », реализующих российской криптографические механизмы, описанные в документах национальной системы стандартизации Российской Федерации;
- создание квантовых систем связи Союзного государства. В 2020 году в Российской Федерации Правительственной комиссией по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности под председательством заместителя Председателя Правительства Российской Федерации одобрена дорожная карта развития высокотехнологичной области «Квантовые коммуникации». В соответствии с указанной дорожной картой к 2024 году в Российской Федерации запланировано развертывание и функционирование семи тысяч километров квантовых сетей, построенных на базе

сертифицированных средств квантовых коммуникаций, реализующих стандартизированные решения.

По нашему мнению, перспективные направления развития высокотехнологичных информационных систем и телекоммуникационных сетей Союзного государства целесообразно строить на базе «проверенных на национальном уровне» информационных технологий, в том числе в области криптографической защиты информации. В рамках Союзного государства совместные защитные технологии целесообразно развивать на базе технологий, определяемые в межгосударственных стандартах в области криптографии и безопасности информационных технологий, описываемые технологии в которых должны быть пройти апробацию на национальном уровне и быть одобрены и приняты его научным сообществом. Российское криптографическое сообщество нацелено на создание стойких криптографических решений, базирующихся на открытых принципах их синтеза для различных отраслей промышленности, что создает условия для вариативного выбора методов криптографической защиты информационных систем и телекоммуникационных сетей. Развитие таких межгосударственных стандартов, в том числе, в области криптографической защиты информации, целесообразно реализовывать на базе Межгосударственного совета по стандартизации, метрологии и сертификации СНГ на паритетных началах через придание соответствующего статуса как российским, так и белорусским стандартизируемым решениям.

Список литературы

1. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».
2. ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе ассиметричных криптографических алгоритмов».
3. ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».
4. ГОСТ 34.310-95 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе ассиметричных криптографических алгоритмов».
5. ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хэширования».
6. ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
7. ГОСТ 34.310-2004 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
8. RFC 4357 «Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001 and GOST R 34.11-94 Algorithms».
9. RFC 4490 «Using the GOST 28147-89, GOST R 34.10-94, GOST R 34.11-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)».
10. RFC 4491 Using the GOST 28147-89, GOST R 34.10-94, GOST R 34.11-94, and GOST R 34.10-2001 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile».
11. RFC 5830 «GOST 28147-89: Encryption, Decryption and Message Authentication Code (MAC) Algorithms».
12. RFC 5831 «GOST R 34.11-94: Hash Function Algorithm».
13. RFC 5832 « GOST R 34.10-2001: Digital Signature Algorithm».
14. ISO/IEC 14888-3 «Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms».

15. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
16. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».
17. ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры».
18. ГОСТ Р 34.13-2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».
19. ISO/IEC 10116 «Information technology – Security techniques – Modes of operation for an n-bit block cipher».
20. ISO/IEC 9797-1 «Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher».
21. ГОСТ 34.10-2018 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
22. ГОСТ 34.11-2018 «Информационная технология. Криптографическая защита информации. Функция хэширования».
23. ГОСТ 34.12-2018 «Информационная технология. Криптографическая защита информации. Блочные шифры».
24. ГОСТ 34.13-2018 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».
25. RFC 6986 «GOST R 34.11-2012: Hash Function».
26. RFC 7091 «GOST R 34.10-2012: Digital Signature Algorithm».
27. RFC 7801 «GOST R 34.12-2015: Block Cipher “Kuznyechik”».
28. RFC 8891 «GOST R 34.12-2015: Block Cipher “Magma”».
29. ISO/IEC 10118-3 «Information technology – Security techniques – Hash functions – Part 3: Dedicated hash-functions».
30. RFC 9189 «GOST Cipher Suites for Transport Layer Security (TLS) Protocol Version 1.2».
31. RFC 9227 «Using GOST Ciphers in the Encapsulating Security Payload (ESP) and Internet Key Exchange Version 2 (IKEv2) Protocols».
32. RFC 7836 «Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.10-2012».
33. RFC 8133 «The Security Evaluated Standardized Password-Autenticated Key Exchange (SESPAKE) Protocol».
34. RFC 8645 «Re-keying Mechanisms for Symmetric Keys».
35. RFC 9058 «Multilinear Galois Mode (MGM)».
36. RFC 9215 «Using GOST R 34.10-2012 and GOST R 34.11-2012 Algorithms with the Internet X.509 Public Key Infrastructure».
37. «Основные направления реализации положений Договора о создании Союзного государства на 2021 – 2023 годы» утверждены Декретом Высшего Государственного Совета Союзного государства от 4 ноября 2021 года № 6.
38. «Положение о требованиях к обеспечению защиты информации при осуществлении перевода денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении денежных средств» утверждено Центральным Банком Российской Федерации от 4 июня 2020 года № 719-П.
39. «Правила предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности)» утверждены Постановлением Правительства Российской Федерации от 19 июня 2020 г. № 890.

УДК 621.381.8.004

ОЦЕНКА ОШИБКИ РАВНОМЕРНОГО КВАНТОВАНИЯ ПЕРИОДИЧЕСКОЙ ПОСЛЕДОВАТЕЛЬНОСТЬЮ ИМПУЛЬСОВ ТРЕУГОЛЬНОЙ ФОРМЫ

[1]В.К. ЖЕЛЕЗНЯК, [1]К.Я. РАХАНОВ, [1]С.В. ЛАВРОВ, [1]Е.Р. АДАМОВСКИЙ,
[1]С.В. ХАРЧЕНКО, [2]А.Г. ФИЛИППОВИЧ, [2]М.М. БАРАНОВСКИЙ
[1]Полоцкий государственный университет, г. Новополоцк, *211440,* Республика Беларусь
[2]Оперативно-аналитический центр при Президенте Республики Беларусь, г. Минск, Республика Беларусь

Введение. Аналоговые речевые сигналы для передачи в высокоскоростных широкополосных каналах связи должны быть представлены в дискретно-квантованном виде. Возникающие при соответствующем преобразовании искажения сигнала требуется оценить в контексте защищенности информации в каналах утечки. Мерой является величина нормативного показателя, ее установление – цель защищенности канала от утечки информации.

Работа посвящена разработке метода имитационного моделирования для оценки защищенности в каналах утечки информации (КУИ) в шумах высокого уровня дискретно-квантованным представлением речевых сигналов.

При оценке возникают погрешности различного характера: алгоритмическая, аппаратурная, статистическая. Применение имитационной модели в локальной измерительной схеме сводит аппаратурную погрешность до уровня точности представления чисел с плавающей запятой средствами вычислительной техники (СВТ).

Основная часть. Развитие средств передачи информации приводит к возрастанию объемов, дальности, качества и верности передачи, что требует высокой помехозащищенности и помехоустойчивости каналов связи, что в большей степени обеспечивается передачей цифровых сигналов.

Принцип формирования цифровых сигналов заключается в разбиении непрерывного аналогового сигнала $x(t)$ на дискретные отсчеты в моменты времени $t = mT$ путем умножения на немодулированные периодические последовательности δ-функций [1] (замена непрерывного сигнала дискретными значениями по уровню и времени – квантование):

$$\delta_T^{'}(t) = \sum_{-\infty}^{\infty} \delta(t - mT)\,. \qquad (1)$$

Дискретные равноотстоящие друг от друга значения сигнала $x(t)$ при $t = mT$ формируют $y(mT)$, и не реагируют на $z(mT)$. Тогда дискретное значение сигнала $x(t)$ представляют как:

$$x(mt) = y(mT) - z(mT), \qquad (2)$$

где $y(mT)$ – δ-функция, импульсы единичной амплитуды и малой длительности;
$z(mT)$ – непрерывная часть сигнала между дискретными моментами.

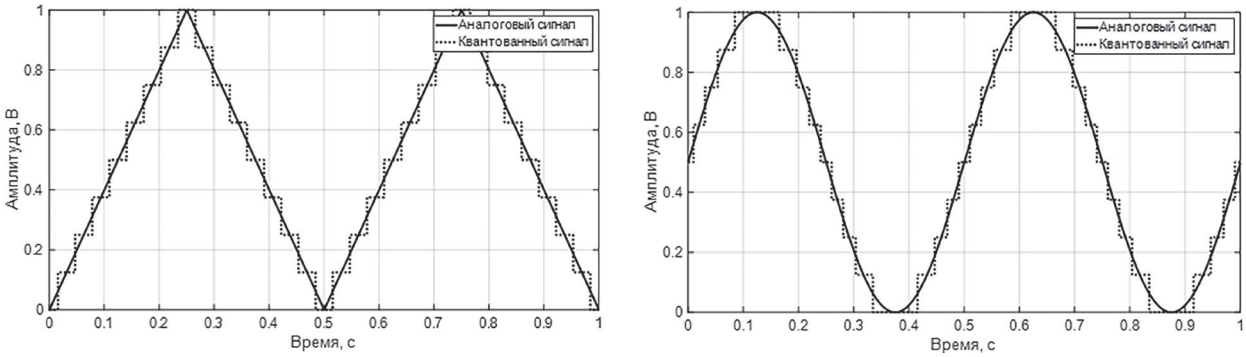
Квантование соответствует выделению значений сигнала в фиксированные моменты времени (интервал квантования), и заменяет непрерывную функцию решетчатой функцией, которая определяется совокупностью выделенных ординат (дискрет), модулирующих последовательность импульсов. Квантование и модуляция осуществляются импульсным

модулятором, входной величиной которого является непрерывный сигнал, а выходной – модулированная последовательность импульсов.

В работах [2-4] предложено использовать сложный измерительный (тестовый) композитный сигнал в виде периодической импульсной последовательности треугольной формы, требования к которому определяются особенностями дискретно-квантованного представления речевых сигналов.

Периодическая последовательность импульсов треугольной формы (рис. 1а) имеет преимущество перед гармоническим измерительным сигналом (рис. 1б) в процессе выделения шума квантования, так как позволяет достичь более высокой точности его обработки при линейной амплитудной характеристике квантования и помехоустойчивой структуре, выделяющей слабые сигналы.

$$s_{треуг} = \frac{8}{\pi^2}(\cos(x) + \frac{1}{9}\cos(3x) + \frac{1}{25}\sin(5x) - \frac{1}{49}\sin(7x) + ...). \quad (3)$$

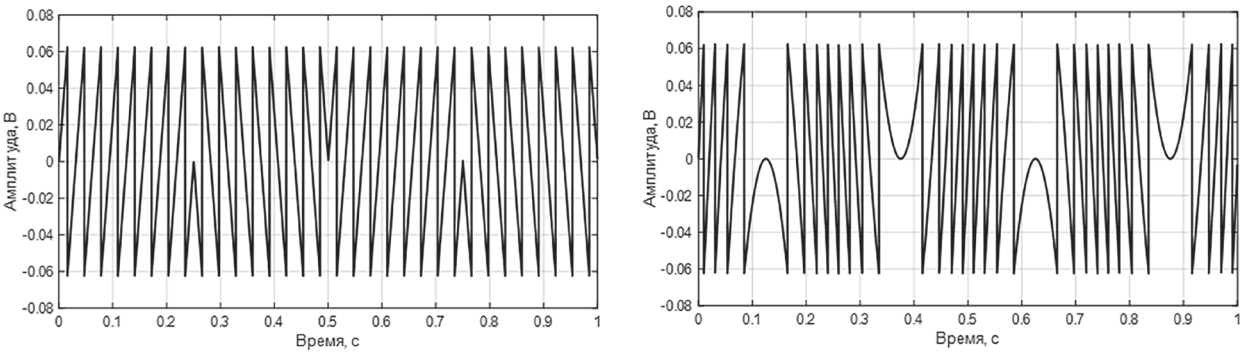


а) б)

Рисунок 1. Квантование последовательностей: а) треугольной; б) гармонической

Шум квантования периодической последовательности импульсов треугольной формы представляет последовательность пилообразных импульсов (рис. 2а), спектральный состав которой включает основную и высшие гармоники. На рис. 2б приведен шум квантования гармонического измерительного сигнала для сравнения.

$$q(s_{треуг}) = \frac{2}{\pi}(\sin(x) - \frac{1}{2}\sin(2x) + \frac{1}{3}\sin(3x) - \frac{1}{4}\sin(4x) + ...). \quad (4)$$



а) б)

Рисунок 2. Шум квантования последовательностей: а) треугольной; б) гармонической

Характеристика квантования $\Phi(x)$ представляется в виде суммы линейной характеристики x и нелинейной ограниченной характеристики $\delta\Phi(x)$ [5]:

$$\Phi(x) = x + \delta\Phi(x),\ \delta\Phi(x) \le x/2 \quad (5)$$

где x – шаг квантования.

Ступенчатая амплитудная характеристика $s' = \varphi(s)$ также представляется в виде суммы идеальной (линейной) характеристики и характеристики, определяющей нелинейные искажения сигнала при равномерном квантовании [1]. При заданной длине кода n максимальное число уровней квантования $N = 2^n$. Диапазон речевого сигнала равен $2U_{max}$, поэтому в N-разрядном квантователе шаг Δ составляет:

$$\Delta = \frac{2U_{max}}{N} = \frac{2U_{max}}{2^n} = U_{max} \times 2^{-n} \quad (6)$$

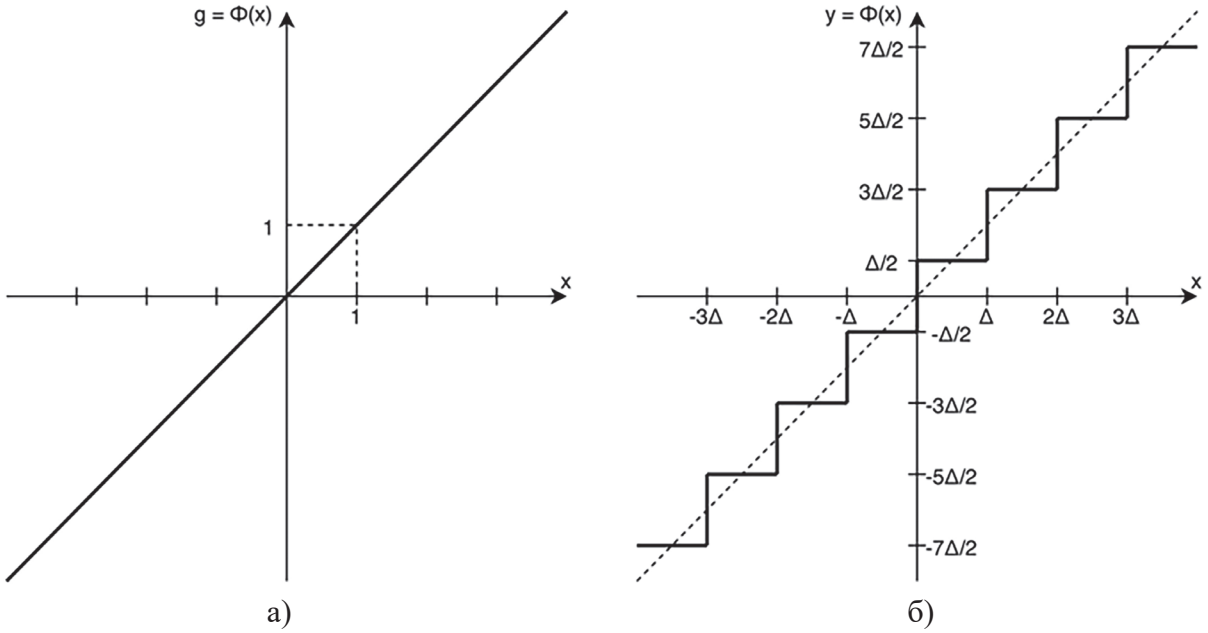
Амплитудная характеристика квантователя представлена на рис. 3а [6] в двухкоординатной системе с равномерной величиной шага квантования и амплитудой в диапазоне [U_{min}... U_{max}]. При двоичном квантовании кодовая группа состоит из импульсов с возможным числом уровней квантования 2^n и шага квантования Δ.

Дискретные уровни принимают значения $\pm 0{,}5\Delta \times (2^n - 1)$ с изменением входного сигнала в пределах до $\Delta \times (2^n - 1) = U_{max} - \Delta$ (рис. 3б). Ошибка между входным аналоговым сигналом и квантованным сигналом является шумом квантования. Ошибка квантования определяется в пределах $|q(s) \le 0{,}5\Delta$ и ограничена ошибкой $\delta^2 = \Delta^2/12$ [7].

В полосах равной разборчивости отношение сигнал/шум (ОСШ) при равномерном квантовании зависит от длины кодовых слов N, частоты дискретизации f_d и ширины полосы Δf_i:

$$ОСШ = 6{,}02N + 10\lg(\frac{f_d}{\Delta f_i}) + C_s \quad (7)$$

где C_s – константа, зависит от формы сигнала и лежит в диапазоне -15… +2 дБ.
i – номер полосы равной разборчивости, от 1 до 20.



а) б)

Рисунок 3. Параметры квантования: а) линейный элемент; б) амплитудная характеристика

Любая измеряемая изменяющаяся величина может быть представлена в виде пачки выборок, разделенных одинаковыми интервалами времени. Значения функции $a(t)$ записываются через интервалы T секунд. Шэннон установил, что эти выборки содержат всю информацию о функции $a(f)$, если описывающий ее спектр частот меньше, чем $1/T$ Гц. Спектр $a(t)$ должен укладываться в полосу частот $\pm 1/2T$, теорема о выборках [8]. Иными словами, если условие Шэннона соблюдено, функция $a(T)$ может быть точно восстановлена по пачке выборок путем свертки выборочной функции $a_s(t) = a(nT)$ с функцией $\sin(\pi t/T)/(\pi t/T)$.

Этот процесс может быть аналитически записан следующим образом:

$$a(t) = a_s(t) \otimes \sin c\left(\frac{t}{T}\right) = \sum_{n=0}^{\infty} a(nT) \sin c\left(\frac{t-nT}{T}\right) \tag{8}$$

Выборочная функция имеет вид:

$$a_s(t) = \sum_{n=0}^{\infty} a(nT)\delta(t-nT) \tag{9}$$

Функция Вудворда sinc:

$$\sin c\left(\frac{t}{T}\right) = \frac{\sin(\pi t/T)}{\pi t/T} \tag{10}$$

Аналоговое напряжение сигнала должно быть квантовано и подвергнуто кодированию при обработке в цифровом виде. В процессе квантования появляются систематические и случайные ошибки.

Идеальным квантующим устройством является нелинейное устройство с нулевой памятью. Интервалы квантования входного сигнала Δ находятся в однозначном соотношении с кодированным выходным цифровым сигналом. Точки перехода разделены одинаковыми интервалами и жестко зафиксированы. Реальные квантующие устройства вносят дополнительные ошибки, обусловленные недостаточно совершенными электрическими или механическими параметрами. Наиболее серьезными являются ошибки: шумовые и калибровки.

Шумовая ошибка появляется из-за нестабильности уровней перехода, обычно независимой от одной выборки к другой. Ошибка калибровки является следствием неизменной нелинейности передаточной характеристики квантующего устройства. Она обычно определяется производственными допусками либо пределами, обусловленными ошибками при юстировке, и часто зависит от таких условий внешней среды, как температура и влажность.

При проектировании конкретных кодирующих устройств такие ошибки ограничивают количество возможных уровней квантования, что определяет количество разрядов в кодированной выборке. Из рис. 4 показано, как уменьшается среднеквадратичное значение ошибки при увеличении числа разрядов в кодирующем устройстве с фиксированной шумовой ошибкой и ошибкой калибровки [9].

Дополнительно исследована зависимость среднеквадратичной погрешности периодической треугольной последовательности от числа k составляющих ее гармоник, которые последовательно удалялись при помощи фильтра с уменьшающейся верхней частотой. Получено, что, при наличии, хотя бы, 5 гармоник, ошибка сигнала составляет менее 1%.

В зависимости нелинейности амплитудной характеристики системы передачи входного сигнала распределение спектральной плотности выходного сигнала деформировано. При подаче на вход сигнала со сложным спектром, выходной спектр системы передачи обогащается новыми частотными составляющими по сравнению с входным сигналом. Ряд причин рассмотрен в работе [2].

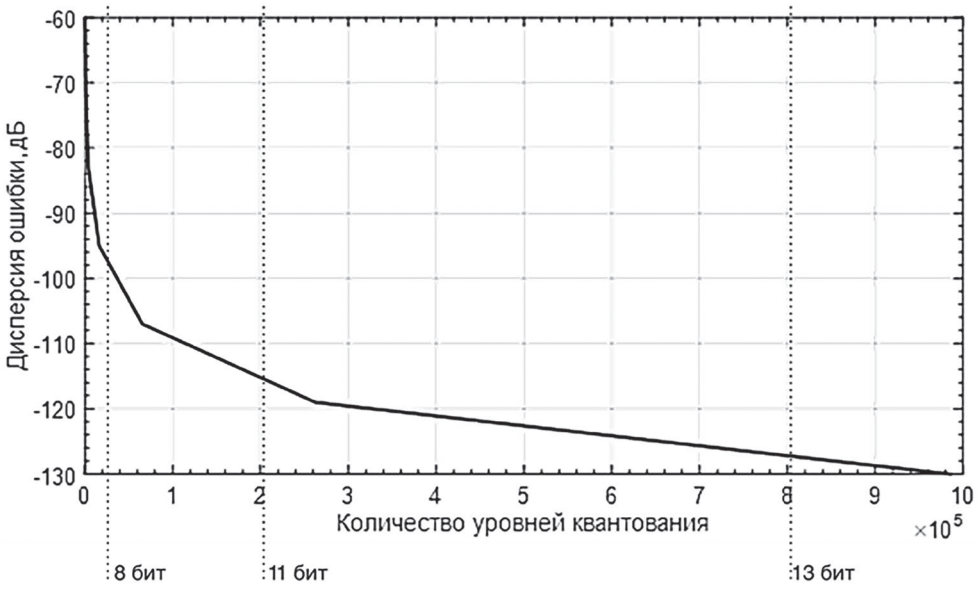


Рисунок 4. Зависимость величины ошибки квантования от разрядности АЦП

Первичным преобразователем снимают поля рассеяния выходного сигнала ЦАП, обрабатывают и усиливают. Выделяют искаженные сигналы в виде периодической последовательности импульсов пилообразной формы, из спектра которых выделяют основные и высшие гармонические составляющие, соответствующие суб-гармоникам и частоте дискретизации, высшим гармоникам частоты дискретизации, а также спектральные составляющие, не соответствующие суб-гармоникам частоты дискретизации $mf_d \pm nf_{треуг}$, $mf_d \pm nf_{пилообр}$.

Нелинейность амплитудной характеристики передающей системы при подаче на вход передаваемого сигнала обуславливает появление на выходе спектральных составляющих, отсутствующих во входном сигнале. При подаче на вход речевого сигнала, имеющего сложный и непрерывно меняющийся во времени спектр, выходной сигнал определяется спектром входного сигнала, диапазоном частот, спектральным распределением продуктов нелинейности, видом нелинейности, амплитудно-частотными характеристиками передающей системы, изменения уровня входного сигнала. Эти объективные факторы определяют деформацию распределения продуктов нелинейности.

Субъективное восприятие продуктов нелинейности определяется чувствительностью уха в диапазоне частот, степенью маскировки продуктов нелинейности полезным сигналом, шумами окружающей среды и передающей системы. Методы оценки нелинейных искажений в полной мере определяются перечисленными факторами. Результаты измерений определяются параметрами сигнала и пиковыми амплитудными характеристиками системы передачи.

Одночастотный измерительный сигнал обуславливает на выходе наличие основной и высших гармоник при аналитическом выражении амплитудной характеристики двумя членами степенного полинома [10].

$$U_{вых} = a_1 U^1{}_{вх} + a_2 U^2{}_{вх} + a_3 U^3{}_{вх} + \ldots \quad (11)$$

При подаче двухчастотного периодического сигнала с гармоническими составляющими $U_{вх} = U_{1вх}\sin(\omega_1 t + \varphi_1) + U_{2вх}\sin(\omega_2 t + \varphi 2) + \ldots$ выходной сигнал содержит синусоидальные колебания частот ω_1 и ω_2 с измененными амплитудами и комбинационными составляющи-

ми, частоты которых содержат суммарные и разносные частоты ($\omega_1 \pm \omega_2$), что показано на рис. 5.

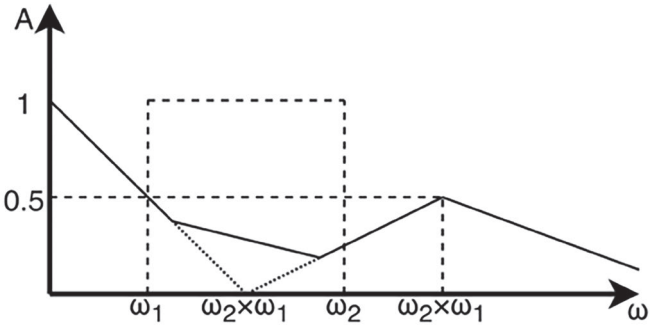


Рисунок 5. Спектральное распределение продуктов нелинейности

На рис. 6 представлены измерения магнитного поля, создаваемого внешним модулем преобразования в режиме ЦАП при обработке тестового сигнала с частотой, соответствующей суб-гармонике (12.5 кГц = $1/5 f_d$), и не соответствующей ей (12.38 кГц). Частоты отстоят друг от друга менее чем на 1%, и в области низких частот могут быть сопоставлены друг с другом [11]. Внешние помехи были исключены за счет измерений в экранированном помещении.

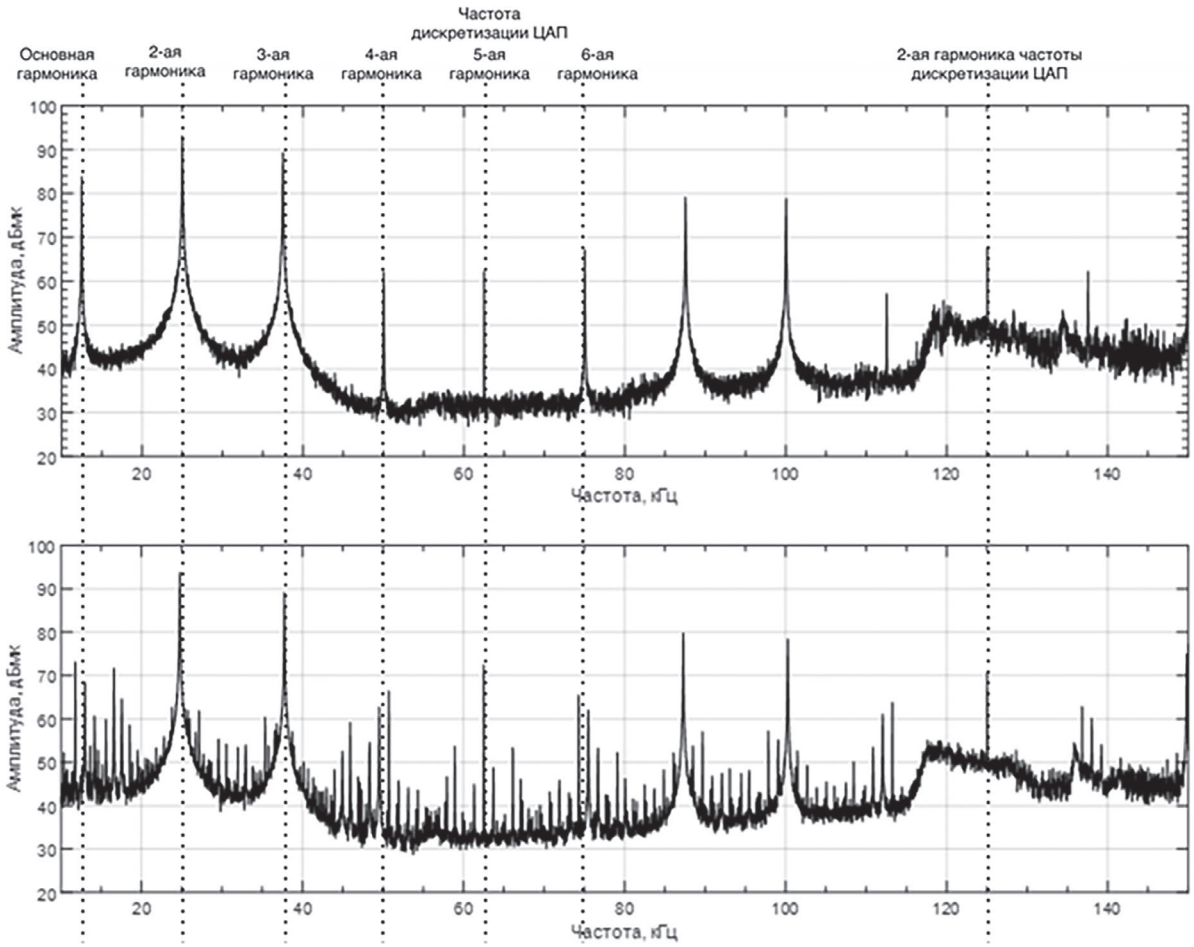


Рисунок 6. Магнитное поле ЦАП при обработке тестового сигнала

В работе [12] рассматривается прохождение сложного сигнала в системе «запись-воспроизведение» при учете нелинейности системы и наличия периодической амплитудной и частотной модуляций.

Для упрощения расчетов коэффициенты четных членов полинома приняты равными нулю при оценке нелинейных искажений полиномом с нечетными степенями, что допустимо для понимания сложности процессов:

$$U_{вых} = a_1{}^1U_{вх} - a_3{}^3U_{вх} + a_5{}^5U_{вх}; \quad (12)$$

где $U_{вх}$, $U_{вых}$ – напряжения на входе и выходе системы;
a – коэффициенты полинома.

Работа [2] в полной мере показывает невозможность оценки искажения квантования, так как спектры гармонических искажений, обусловленные высшими четными и нечетными гармониками, комбинационными искажениями различных порядков комбинаций.

Использование измерительного сигнала периодической последовательности импульсов не вносит методических погрешностей при оценке защищенности каналов утечки, обусловленных нелинейностью шума квантования. В работе [10] представлены результаты, определяющие типовые амплитудные характеристики системы передачи и количество измерительных гармонических сигналов, используя амплитудную характеристику при аналитическом выражении тремя членами ступенчатого полинома.

Заключение. Впервые предложено с высокой точностью оценивать шум квантования гармоническим сигналом вместо узкополосного шума для оценки по единой методике для аналоговых и цифровых речевых сигналов.

В качестве источника измерительного сигнала предложена периодическая последовательность импульсов треугольной формы, в результате чего искажения при квантовании не содержат погрешностей, обусловленных измерительным сигналом.

Периодическая последовательность импульсов пилообразной формы включает основную, высшие четные и нечетные гармоники; аналитически описывается с помощью полинома с основной и высшими четными и нечетными гармониками. При подаче на вход полиномом несколько гармонических сигналов, на выходе образуются сигналы с исходными частотами и измененными амплитудами и комбинационные составляющие различных порядков.

Список литературы

1. Цыпкин Я.З. Основы теории автоматических систем. М.: Наука, 1977. 560 с.
2. Некоторые проблемы оценки защищенности шума квантования / В.К. Железняк [и др.] // Проблемы инфокоммуникаций. 2020. № 2-2(12). С. 60-65.
3. Способ оценки защищенности преобразованного в цифровую форму речевого сигнала: пат. BY № 23689, Железняк В.К., Лавров С.В., Филиппович А.Г., Барановский М.М.; заявл. 04.12.2019.
4. Железняк В.К., Лавров С.В., Барановский М.М., Филиппович А.Г. Способ оценки защищенности преобразованного в цифровую форму речевого сигнала в каналах утечки информации // Комплексная защита информации: материалы XXIV научно-практической конференции. Витебск. 2019. С. 53-59.
5. Передача информации в системах подвижной связи / В.Ю. Бабков [и др.]. СпбГУТ. 1999. 152 с.

6. Шелухин, О.И., Лукьянцев Н.Ф. Цифровая обработка и передача речи / Москва: Научно-техническое издательство «Радио и связь». 2000. 456 с.
7. Мирский Г.Я. Характеристики стохастической взаимосвязи и их измерения. М.: Энергоиздат. 1982. 320 с.
8. Woodward P. M. Probability and Information Theory, with Application to Radar. New York: McGraw-Hill Book Company, 1953. 146 p.
9. Гольденберг Л.М., Матюшкин Б.Д., Поляк М.Н. Цифровая обработка сигналов: Справочник. М.: Радио и связь. 1985. 312 с.
10. Бабуркин В.Н., Гензель Г.С., Павлов Н.Н. Электроакустика и радиовещание. Акустические вопросы вещания: учебное пособие. Москва: Связь. 1967. 312 с.
11. Железняк В.К., Раханов К.Я., Лавров С.В., Адамовский Е.Р., Барановский М.М., Филиппович А.Г. Спектральное представление сигнала ошибки равномерного квантования периодической импульсной последовательностью треугольной формы // Материалы XXVI Междунар. науч.-техн. конф. «Современные средства связи», Минск. БГАС. 2021.
12. Железняк, В.К. Спектральный состав выходного сигнала в системе запись-воспроизведение при одновременном воздействии амплитудной и частотной модуляции // Вопросы радиоэлектроники. Серия, Общетехническая. 1967. №13. С. 31-52.

УДК 004.056.53

МЕТОДЫ УСИЛЕННОЙ АУТЕНТИФИКАЦИИ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ

Р. В. МЕЩЕРЯКОВ, А.Ю. ИСХАКОВ, С.Ю. ИСХАКОВ
Федеральное государственное бюджетное учреждение науки
Институт проблем управления им. В. А. Трапезникова Российской академии наук,
г. Москва*, 117997,* Российская Федерация

Введение

Динамика последних событий в мире информационной безопасности свидетельствует о серьезной трансформации методов и технологий совершения атак на промышленные киберфизические системы, зачастую с использованием средств маскирования злоумышленных действий под видом легитимных операций. Наиболее отчетливо это проявляется в части механизмов аутентификации, поскольку опознавательные характеристики, применяемые для установления подлинности пользователя, могут быть скомпрометированы. В то же время отставание темпов развития тактик защиты от стремительного повышения квалификации злоумышленников приводит к масштабной проблеме выявления ранее неизвестных атак, при которых угрозы невозможно формализовать и/или описать определенными сигнатурами.

Политики безопасности, основанные на статических правилах однофакторных и многофакторных алгоритмов проверки, не только приводят к строгим ограничениям, затрудняющим оперативное управление киберфизическими системами, но и имеют ряд существенных недостатков, связанных с тем, что для установления подлинности пользователя применяются опознавательные характеристики, которые могут быть скомпрометированы злоумышленниками.

1. Особенности интеграции в киберфизические системы

Глубокий уровень взаимодействия между физическими и вычислительными элементами киберфизических систем в целом обеспечивает возможность применения существующих средств контроля и управления доступом в программно-аппаратных комплексах. Однако к числу отличительных особенностей подавляющего большинства решений для киберфизических систем являются высокие требования к уровню функционирования, безопасности и надежности протоколов управления, а также необходимость сочетания многопрофильных задач в рамках одного производственного процесса, ведения непрерывного мониторинга и анализа состояния системы [1]. Перспективные направления адаптации методов и алгоритмов защиты информации для их использования в киберфизических системах зачастую обусловлено низкой вычислительной способностью компонентов таких комплексов.

К числу особенностей, которые следует учитывать при интеграции систем аутентификации следует также отметить высокий уровень доверия между субъектами (в случае систем промышленной автоматизации, АСУ ТП и т.д.), невозможность свободной реализации блокирующих функций пользователей при фиксации попыток несанкционированного получения доступа в связи с повышенными требованиями к обеспечению доступности и целостности. Эти особенности затрудняют применимость современных алгоритмов, методов и средств обеспечения безопасности.

При этом, ландшафт угроз и уязвимостей, характерных для применяемого в киберфизических системах широкого спектра аппаратных и программных технологий, чрезвычайно широк и сложен.

2. Современные решения в области идентификации и аутентификации

Традиционные методы идентификации и аутентификации, основанные на использовании явных способов проверки, имеют ряд существенных недостатков, связанных с тем, что для установления подлинности пользователя применяются опознавательные характеристики, которые могут быть скомпрометированы злоумышленниками. Для снижения рисков компрометации пользовательских учетных записей разработчики повсеместно стараются внедрять решения, основанные на многофакторных алгоритмах проверки подлинности [1-2]. Однако эта парадигма защиты основана на статических правилах и приводит к строгим ограничениям вне зависимости от личности пользователя и реальных рисков [3]. В связи с этим, множество научных исследований в области теории защиты информации сегодня сопряжено с разработкой новых методов в области риск-ориентированной аутентификации. Эта концепция подразумевает, что у любого фактора аутентификации есть уровень доверия, а выбор фактора аутентификации зависит от уровня риска конкретной операции. Такие решения безусловно являются крайне важными и актуальными. С одной стороны, они обеспечивают возможность обезопасить пользователя от компрометации учетной записи путем анализа активности его профиля на предмет аномальных характеристик, с другой стороны – подобрать баланс между удобством и надежностью, обеспечив в некоторых случаях возможность уменьшить количество процедур аутентификации. Поведенческий анализ пользователей и сущностей как процесс кибербезопасности для детектирования внутренних угроз, атак или мошенничества, обрел высокую популярность среди вендоров и специалистов в сфере информационной безопасности [4]. Причины появления таких решений довольно очевидны. Стремительными темпами увеличиваются объемы информации, циркулирующей в корпоративных сетях, глобальном информационном пространстве. Растет уровень компетенций злоумышленников, а атаки, которые изо дня в день проводятся

с целью хищения информации или ее модификации в информационных системах, принимают все более завуалированный вид. Их становится крайне сложно отличить от штатного, легитимного поведения пользователей. Совокупность вышеперечисленных факторов привела к появлению нового класса решений, UEBA-модулей информационной безопасности [5]. В современной литературе выделяется целый ряд различных поднаправлений поведенческого анализа действий пользователей: User Behavioral Analytics (UBA); Security User Behavior Analytics (SUBA); User and Entity Behavior Analytics (UEBA).

В работе [6] предлагается реализация системы адаптивной аутентификации базе Байесовской сети. Авторы предлагают использовать следующие компоненты, характеризующие основные параметры пользователя: CUSIM = (Real User, Location, KD, IP, CU-SIM, PDT). Вес каждого из ребер между элементами данных компонентов основан на вероятности того, что авторизацию осуществляет реальный пользователь, учитывая зависимости между данными событиями. Если известна структура модели Байесовской сети и доступна полная выборка данных, можно проверить распределение вероятностей путем вычисления статистики из выборок данных, воспользовавшись непосредственно теоремой Байеса. Согласно [7], можно применять Байесовские сети и для изучения стратегий вторжения. Целью компонента, предлагаемого в данной работе, является извлечение шаблонов действий атаки, которые впоследствии будут использоваться для корреляции предупреждений во время выполнения. Здесь автоматически генерируются правила корреляции, анализируя ранее наблюдаемые предупреждения, используя метод Байесовской сети. В работе [8] рассмотрен метод аутентификации с применением расстояния Хаусдорфа на основе дистанционной модели для IP-цепей в сервисно-ориентационной среде интернета вещей. Путем сопоставления характеристики можно найти реальные позиции идентификационных данных для аутентификации, и предлагается метод для вычисления расстояния Хаусдорфа. Предложенный метод может преобразовать вычисление расстояния в минимальное расстояние между двумя точками. В результате эффективность и стабильность метода улучшаются. Еще один подход анализа данных пользователя, согласно [9], сочетание преобразования кривой Гильберта и сети Вороного. Одним из идентификационных признаков в данной модели является местоположение пользователя. Предлагаемая система обеспечивает лучшие результаты, поскольку информация о местонахождении не попадает к неавторизованным пользователям сети. Для получения данных в соответствии с запросом пользователя используют алгоритм классификации RK-NN — обратный “метод ближайших соседей”. Тем не менее, несмотря на наличие проприетарных разработок и отдельных исследований по обеспечению безопасности информационных систем с помощью адаптивных алгоритмов, в данной области имеется ряд проблем.

Первая проблема связана с невозможностью их применения в аспекте идентификации субъектов киберфизических систем, зачастую маскирующих свои действия под выполнения сервисных процедур. Многие исследователи ставят своей целью определить рациональное признаковое пространство, которое позволит достоверно идентифицировать посетителей по их косвенным характеристикам (параметрам рабочей среды) или с помощью обработки статистических данных поведенческих параметров (методы динамической биометрической аутентификации).

Широкую популярность приобрели методы фингерпринтинга (fingerprinting). Активно разрабатываются различные алгоритмы, методы и технологии для достижения новых результатов в данной области. Например, в [10–12] рассматриваются вопросы выявления посетителя интернет-ресурса по базовому набору особенностей используемого браузера.

Исследование [13] посвящено повышению степени достоверности идентификации субъекта за счет анализа вспомогательной мета-информации о массиве свойств программного обеспечения пользователя. К числу параметров, формирующих наиболее знаковое признаковое пространство [14] относят: список установленных шрифтов, набор плагинов браузера, предоставляемый при помощи JavaScript, информацию о локализации ОС, SuperCookie, параметрическую информацию об отрисовке при помощи элемента Canvas (Canvas fingerprinting) и др.

Ассимиляция вышеперечисленной информации наиболее эффективным образом позволяет сформировать в базе данных системы идентификации уникальный отпечаток компьютера [15]. В 2010 году Фонд электронных рубежей измерил более чем 18,1 бита информационной энтропии, возможной для фингерпринта. Однако это исследование было до изобретения цифрового отпечатка с использованием Canvas, который добавил еще 5,7 бита. В 2017 был опубликован метод кроссбраузерного фингерпринта [16, 17], позволяющий следить за пользователем из разных браузеров на одном устройстве.

Несмотря на то, что в подобных работах предлагается использовать кортеж наиболее значимых по мнению их авторов признаков для идентификации, отсутствует проведение единого корреляционного анализа всех признаков, который позволил бы выявить зависимости между ними и оптимизировать признаковое пространство. Учитывая, что многие обнаруженные информативные метрики определяются вычислительно-сложными методами, подобные подходы не находят широкого распространения ввиду необходимости сохранения быстрого отклика веб-ресурса.

Следует отметить, что упомянутые техники эффективны только для обычных web-браузеров, не претендующих на функционал по обеспечению анонимности пользователей. В специализированных браузерах, таких как Tor Browser, большинство разрабатываемых методов оценки особенностей аппаратного и браузерного окружения блокируются [18]. А, учитывая, что данное исследование направлено на развитие методов противодействия подготовленному злоумышленнику, априори применяющему инструменты для регулярной смены отпечатков браузера, технологии фингерпринтинга можно применять только в совокупности с дополнительными механизмами идентификации.

Системы идентификации, основанные на базе синтаксического и морфологического анализа текстовых данных, индексирующие сообщения пользователей с определенными ключевыми словами, не могут быть применены в исследуемых объектах в связи с их характерными особенностями (большинство субъектов в процессе взаимодействия с интерфейсом управления киберфизической системы заполняет минимальные объемы текстовых данных). Алгоритмы аутентификации субъектов по клавиатурному почерку по той же причине не могут применяться в выбранной предметной области. Существуют подходы, опирающиеся на возможность учета особенностей работы с манипулятором типа мышь для идентификации его владельца, например, [19–22]. В работе [23] автор определяет пользователя компьютерной игры, на основе обученной на исторических данных нейронной сети. Для обработки данных используется машина состояний. Оценивается не только траектория, но и точность кликов. Погрешность ПО составляет 6-20%. В исследовании [24] предлагается использовать биометрические данные, полученные анализом использования мыши для постоянной (периодической) аутентификации пользователя. Биометрия данных движения мыши представляется как отражение психологических и поведенческих характеристик пользователя. Выделяются такие данные, как настроение и усталость. В статье [25] проводится сравнительный анализ методов аналогичных исследований (с точностью иден-

тификации от 84% до 99,7%). В 2017 году исследователи разработали прототип системы, учитывающей скорость движения мышью и особенности прокрутки колесом [26]. Несмотря на большой научный задел в данной отрасли, стоит отметить, что все перечисленные исследования проводились на системах аутентификации, применяемых для решения задачи «свой-чужой».

Среди современных исследований в области информационной безопасности известны работы, посвященные развитию методов проактивного обнаружения угроз, которые невозможно обнаружить традиционными средствами защиты. Результатом подобных процессов являются динамически обновляемые индикаторы компрометации, получение которых основано на анализе больших данных с помощью методов машинного обучения.

Заключение

Таким образом, перспективным прорывным направлением в области риск-ориентированной аутентификации будет развитие механизмов динамического формирования политик проверки легитимности субъектов доступа в киберфизических системах, предполагающих, что роль администратора безопасности в большей степени будет связана с координацией и коррекцией процесса машинного обучения на больших данных системы.

Для решения задачи разработки аппарата адаптивной корректировки методов аутентификации требуется создание классификатора динамически обновляемых индикаторов компрометации и эффективного алгоритма машинного обучения по признакам не только известных, но и ранее не фиксируемых угроз безопасности. На основе анализа современного состояния исследований в выбранной области можно заключить, что в настоящее время не существует комплексного решения, использующего современные технологии и средства, а также соответствующего текущему развитию и нарастающим вызовам обозначенного проблемного вопроса – возможностей эффективного применения методов адаптивной аутентификации в киберфизических системах на основе проактивных алгоритмов обнаружения атак.

Исследование выполнено за счет гранта Российского научного фонда № 22-21-00846.

Список литературы

1. Мещеряков, Р. В., Исхаков, А. Ю., & Евсютин, О. О. (2020). Современные методы обеспечения целостности данных в протоколах управления киберфизических систем. Информатика и автоматизация, 19(5), 1089-1122. https://doi.org/10.15622/ia.2020.19.5.7
2. Shashanka M., Shen M., Wang J. User and entity behavior analytics for enterprise security // 2016 IEEE International Conference on Big Data (Big Data), Washington, DC. 2016. P. 1867-1874
3. Бродский А. Риск-ориентированная аутентификация // BIS Journal. 2018. № 2 (29). https://journal.ibbank.ru/post/665
4. Исхаков А. Ю., Исхакова А. О., Мещеряков Р. В., Бендрау Р., Мелехова О. Использование тепловой карты поведения пользователя в задаче идентификации субъекта инцидента информационной безопасности // Труды СПИИРАН. 2018. № 6 (61). С. 147-171.
5. Котенко, И.В. Выявление инсайдеров в корпоративной сети: подход на безе UBA и UEBA / И.В. Котенко, И.А. Ушаков, Д.В. Пелевин, А.И. Преображенский, А.Ю. Овраменко // Защита информации. Инсайд. – 2019. – № 5(89). – С. 26-35.
6. Chantan, Charoon. Improving Accuracy of Authentication Process via Short Free Text using Bayesian Network // 2012 International Journal of Computer Science Issues.

7. Kavousi, Fatemeh & Akbari, Behzad. A Bayesian network-based approach for learning attack strategies from intrusion alerts. // 2014 Security and Communication Networks. 7. 10.1002/sec.786.
8. Liang, Wei & Huang. Hausdorff Distance Model-Based Identity Authentication for IP Circuits in Service-Centric Internet-of-Things Environment. //Sensors 2019. №19. 487. 10.3390/s19030487.
9. Srilakshmi V., Dhamodharan P. Improved Privacy over Authentication of K-Nearest Neighbor Query on Spatial Network // 2015
10. Eckersley P. How Unique Is Your Web Browser? // Proceedings of the 10th Privacy Enhancing Technologies Symposium (PETS). 2010. P. 1-18.
11. Alnaami K., Ayoade G., Siddiqui A., Ruozzi N., Khan L., Thuraisingham B. P2V: Effective Website Fingerprinting Using Vector Space Representations // 2015 IEEE Symposium Series on Computational Intelligence. 2015. P. 59-66.
12. Iskhakov A., Meshcheryakov R., Iskhakov S., Krainov A. Increase in security of authentication services through additional identification using optimal feature space // Proceedings of the IV International research conference “Information technologies in Science, Management, Social sphere and Medicine” (ITSMSSM 2017). 2017. P.443-446.
13. Бессонова Е.Е., Зикратов И.А., Колесников Ю.Л., Росков В.Ю. Способ идентификации пользователя в сети Интернет // Научно-технический вестник информационных технологий, механики и оптики. 2012. Вып.3. С. 133-137.
14. Usmonov B., Evsutin O, Iskhakov A., Iskhakova A., Shelupanov A., Meshcheryakov R. The cybersecurity in development of IoT embedded technologies // 2017 International Conference on Information Science and Communications Technologies (ICISCT). 2017. Pp. 012056.
15. Исхаков А.Ю., Исхаков С.Ю., Мещеряков Р.В. Повышение защищенности сервисов аутентификации путем проведения дополнительной идентификации с использованием оптимального признакового пространства // Информационные технологии в науке, управлении, социальной сфере и медицине. Сборник научных трудов. 2017. С. 117-122.
16. Abouollo A., Almuhammadi S. Detecting malicious user accounts using Canvas Fingerprint // 2017 8th International Conference on Information and Commu-nication Systems (ICICS). 2017. P. 358-361.
17. Daud N.I., Haron G.R., Othman S.S.S. Adaptive authentication: Implementing random canvas fingerprinting as user attributes factor // 2017 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE). 2017. P. 152-156.
18. Система управления проектами Trac. URL: https://trac.torproject.org/projects/tor/ que-ry?status=accepted&status=assigned&status=needs_review&status=needs_revisi-on&status=new&status=reopened&order=priority&col=id&col=summary&col=keywords&col=status&col=owner&col=type&col=priority&keywords=tbb-fingerprinting
19. Диденко С.М. Исследование модели динамики параметров информационного почерка пользователя // Вестник Тюменского государственного уни-верситета. 2006. № 5. С. 170-174.
20. Pilankar P.S., Padiya P. Multi-phase mouse dynamics authentication system using behavioural biometrics // 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES). 2016. P. 1947-1950.
21. Hu S., Bai J., Liu H.; Wang C., Wang B. Deceive Mouse-Dynamics-Based Authentication Model via Movement Simulation // 2017 10th International Symposium on Computational Intelligence and Design (ISCID). 2017. Vol. 1. P. 482-485.
22. Chen X., Xu F., Xu R., Yiu S.M., Shi J. A practical real-time authentication sys-tem with Identity Tracking based on mouse dynamics // 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). 2014. P. 121-122.
23. Kaminsky R., Enev M., Andersen E. Identifying Game Players with Mouse Biometrics. University of Washington. Technical Report. 2008.

24. Feher C., Elovici Y., Moskovitch R., Rokach L., Schclar A. User Identity Verifi-cation via Mouse Dynamics // Information Sciences. 2012. Vol. 201. P. 19-36.
25. Stanić M. Continuous user verification based on behavioral biometrics using mouse dynamics // Proceedings of the ITI 2013 35th International Conference on Information Technology Interfaces. 2013. P. 251-256.
26. Идентификация пользователей Tor Browser через анализ особенностей работы с мышью. URL: https://www.opennet.ru/opennews/art.shtml?num=44027 (дата обращения 20.06.2019).

УДК 004.421.6: 519.23

ТЕСТИРОВАНИЕ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ЭНТРОПИЙНЫХ ПРОФИЛЕЙ

В.Ю. ПАЛУХА, Ю.С. ХАРИН
НИИ прикладных проблем математики и информатики,
Белорусский государственный университет
г. Минск, 220030, Республика Беларусь

Введение. Генераторы случайных и псевдослучайных последовательностей являются одним из элементов систем криптографической защиты информации (СКЗИ). Стойкость СКЗИ зависит от того, насколько близка генерируемая последовательность по своим свойствам к равномерно распределённой случайной последовательности (РРСП) [1], которая на практике называется «чисто случайной» последовательностью.

Для проверки качества криптографических генераторов используются статистические тесты, в которых проверяется гипотеза $H_* = \{\{x_t\}$ является РРСП$\}$ о том, что наблюдаемая последовательность $\{x_t\}$ является равномерно распределённой случайной последовательностью. В качестве тестовой статистики целесообразно использовать статистические оценки энтропии [2]. Одними из самых распространённых функционалов энтропии являются функционалы Шеннона, Реньи и Тсаллиса, которые и будут рассмотрены в дальнейшем.

Оценки энтропии**.** Пусть на вероятностном пространстве (Ω, F, P) с множеством состояний $\Omega = \{\omega_1, \ldots, \omega_N\}$ определена случайная величина $x = x(\omega) = \omega$ с дискретным распределением вероятностей $p = \{p_k\}$, $p_k = P\{x = \omega_k\}$, $p_k \geq 0$, $\sum_{k=1}^{N} p_k = 1$, $k = 1, \ldots, N$. В таблице 1 приведены формулы наиболее распространённых функционалов энтропии.

Таблица 1. Функционалы энтропии:

Энтропия Шеннона	$H(p) = -\sum_{i=1}^{N} p_i \ln p_i$
Энтропия Реньи	$H_r(p) = \frac{1}{1-r} \ln\left(\sum_{i=1}^{N} p_i^r\right), \quad r \in \mathbb{N}, r > 1.$
Энтропия Тсаллиса	$S_r(p) = \frac{1}{r-1}\left(1 - \sum_{i=1}^{N} p_i^r\right), \quad r \in \mathbb{N}, r > 1.$

Пусть имеется случайная последовательность $\{x_t : t = 1, \ldots, n\}$ объёма n из распределения вероятностей $\{p_k\}$, по которой будет оцениваться энтропия. Частотные оценки вероятностей имеют вид

$$\hat{p}_k = \frac{\nu_k}{n}, \quad \nu_k = \sum_{t=1}^{n} I\{x_t = \omega_k\} \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}, \quad I\{x_t = \omega_k\} = \begin{cases} 1, x_t = \omega_k; \\ 0, x_t \neq \omega_k. \end{cases} \tag{1}$$

Рассмотрим асимптотику совместного увеличения объёма выборки и сложности задачи:

$$n, N \to \infty, n/N \to \lambda, 0 < \lambda < \infty. \tag{2}$$

В асимптотике (2) для распределения вероятностей статистик $\{\nu_k\}$ справедлива аппроксимация законом Пуассона $\Pi(\lambda_k)$ с параметром $\lambda_k = np_k$. При истинной гипотезе H_* все элементарные вероятности равны: $p_k = 1/N$, $k = 1..., N$, поэтому все частоты $\{\nu_k\}$ имеют одинаковый параметр распределения Пуассона $\lambda = n/N$.

Оценка энтропии Шеннона на основе частотных статистик (1) имеет вид:

$$\hat{H} = \hat{H}(n, N) = -\sum_{k=1}^{N} \hat{p}_k \ln \hat{p}_k = -\sum_{k=1}^{N} \frac{\nu_k}{n} \ln \frac{\nu_k}{n} = \ln n - \frac{1}{n} \sum_{k=1}^{N} \nu_k \ln \nu_k. \tag{3}$$

Теорема 1 [3]. В асимптотике (2) статистика (3) при гипотезе H_* имеет асимптотически нормальное распределение с параметрами

$$\mu_H = \ln n - e^{-\lambda} \sum_{k=1}^{+\infty} \frac{\ln(k+1)\lambda^k}{k!}, \tag{4}$$

$$\sigma_H^2 = \frac{e^{-\lambda}}{n} \sum_{k=1}^{+\infty} \frac{(k+1)\lambda^k}{k!} \ln^2(k+1) - \frac{e^{-2\lambda}}{N} \left(\sum_{k=1}^{+\infty} \frac{\ln(k+1)\lambda^k}{k!} \right)^2 - \frac{e^{-2\lambda}}{n} \left(\sum_{k=1}^{+\infty} \ln(k+1) \frac{\lambda^k}{k!} (k+1-\lambda) \right)^2. \tag{5}$$

Как следует из теоремы 1, в асимптотике (2) оценка (3) является смещённой, и с уменьшением λ смещение растёт. Для функционалов энтропии Реньи и Тсаллиса можно построить несмещённую оценку в асимптотике (2), в т.ч. и при $\lambda < 1$. Как видно из таблицы 1, эти функционалы являются функциями от величины

$$P_r(p) = \sum_{k=1}^{N} p_k^r. \tag{6}$$

Определим r-ую нисходящую факториальную степень x:

$$x^{\underline{r}} = x(x-1)\ldots(x-r+1) = \frac{x!}{(x-r)!} = \sum_{i=0}^{r} s(r,i) x^i, \tag{7}$$

где $s(r, i)$ – число Стирлинга первого рода; при $x < r$ полагают $x^{\underline{r}} ::= 0$.

Несмещённая оценка для (6) основана на (7) [4]:

$$\tilde{P}_r(p) = \sum_{k=1}^{N} \frac{\nu_k^{\underline{r}}}{n^r}. \tag{8}$$

Полагая, что случайная величина ν имеет распределение Пуассона с параметром λ, т.е. $\mathcal{L}\{\nu\} = \Pi(\lambda)$, получим согласно [5] $E\{\nu^{\underline{r}}\} = \lambda^r$. Кроме того, согласно [5], $E\{\nu^r\} = \sum_{i=0}^{r} S(r,i)\lambda^i$, где $S(r, i)$ – число Стирлинга второго рода.

Статистические оценки энтропии Реньи и Тсаллиса, построенные с использованием оценки (8), имеют вид

$$\hat{H}_r(n, N) = \frac{1}{1-r}\ln\left(\sum_{k=1}^{N}\frac{\nu_k^r}{n^r}\right) = \ln n + \frac{1}{r-1}\left(\ln n - \ln\sum_{k=1}^{N}\nu_k^r\right), \tag{9}$$

$$\hat{S}_r(n, N) = \frac{1}{r-1}\left(1-\sum_{k=1}^{N}\frac{\nu_k^r}{n^r}\right) = \frac{1}{r-1}\left(1-\frac{1}{n^r}\sum_{k=1}^{N}\nu_k^r\right). \tag{10}$$

Теорема 2 [3]. В асимптотике (2) статистика (10) является состоятельной асимптотически несмещённой оценкой энтропии Тсаллиса и при истинной гипотезе H_* имеет асимптотически нормальное распределение с параметрами:

$$\mu_{S,r} = \frac{1}{r-1}\left(1-\frac{1}{N^{r-1}}\right), \tag{11}$$

$$\sigma^2_{S,r} = \frac{\lambda^{r-1}}{(r-1)^2 n^{2r-1}}\left(\sum_{i=1}^{r} s(r,i)\sum_{j=1}^{i-1} C_i^j r^{i-j}\sum_{k=1}^{j} S(j,k)\lambda^k - r^2\lambda^{r-1} + r!\right). \tag{12}$$

Следствие 1. *При $r = 2$ для математического ожидания и дисперсии асимптотического распределения оценки* (10) *справедливы выражения:*

$$\mu_{S,2} = 1-\frac{1}{N}, \quad \sigma^2_{S,2} = \frac{2}{Nn^2}.$$

Теорема 3 [3]. *В асимптотике* (2) *статистика* (9) *является состоятельной оценкой энтропии Реньи и при истинной гипотезе H_* имеет асимптотически нормальное распределение с параметрами:*

$$\mu_{H,r} = \ln N, \tag{13}$$

$$\sigma^2_{H,r} = \frac{\sum_{i=2}^{r} s(r,i)\sum_{j=1}^{i-1} C_i^j r^{i-j}\sum_{k=1}^{j} S(j,k)\lambda^k - r^2\lambda^{r-1} + r!}{(r-1)^2 n\lambda^{r-1}}. \tag{14}$$

Следствие 2. При $r = 2$ для дисперсии асимптотического распределения вероятностей оценки (9) справедливо выражение:

$$\sigma^2_{H,2} = \frac{2}{n\lambda}.$$

Тестирование генераторов. Пусть $\alpha \in (0,1)$ – заданный уровень значимости. Введём обозначения: $\hat{h}$ – статистическая оценка энтропии Шеннона (3), Реньи (9) или Тсаллиса (10), μ_h – асимптотическое математическое ожидание статистической оценки энтропии Шеннона (4), Реньи (13) или Тсаллиса (11), σ_h^2 – асимптотическая дисперсия статистической оценки энтропии Шеннона (5), Реньи (14) или Тсаллиса (12) при истинной гипотезе H_*. Вычислим для наблюдаемой последовательности статистику $\hat{h}$. Решающее правило, основанное на статистике $\hat{h}$, имеет вид [3]:

$$\text{принимается} \begin{cases} H_*, & \text{если } t_- < \hat{h} < t_+; \\ \overline{H_*}, & \text{в противном случае,} \end{cases} \qquad t_\pm = \mu_h \pm \sigma_h \Phi^{-1}\left(1-\frac{\alpha}{2}\right). \tag{15}$$

где $\Phi(\cdot)$ – функция распределения стандартного нормального закона.

Пусть генератор порождает двоичную выходную последовательность $\{y_\tau\}$, $\tau = 1, \ldots, T$. «Нарежем» её на непересекающиеся подряд идущие фрагменты длины s (s-граммы): $X^{(t)} = (X_j^{(t)}) = (y_{(t-1)s+1}, \ldots, y_{ts}) \in \{0,1\}^s$, $t = 1, \ldots, n = [T / s]$. Из полученных s-грамм

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 (15) мы можем вычислить последовательность нормированных отклонений оценки энтропии от математического ожидания в зависимости от s, которые назовём **энтропийными профилями**:

$$\chi(s) = \frac{\hat{h}(s) - \mu_h(s)}{\sigma_h(s)\Phi^{-1}\left(1-\alpha/2\right)}, \; s = 1, \ldots, s_+. \tag{16}$$

Тестирование с помощью профиля позволяет выносить решение о принятии или отклонении гипотезы H_* на основе решающего правила (15) 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.

Представляют теоретический и практический интерес задачи исследования стохастической зависимости статистик $\chi(s)$ в (16). Исследуем зависимость соседних статистик $\chi(s)$ и $\chi(s + 1)$. Для этого вначале исследуем зависимость частотных оценок (1). Пусть $\left\{\hat{p}_i(s)\right\}$ и $\left\{\hat{p}_k(s+1)\right\}$ – частотные оценки (1), вычисленные для s- и $(s + 1)$-грамм соответственно, $i = 0, \ldots, 2^s - 1, k = 0, \ldots, 2^{s+1} - 1$. Справедлива следующая теорема о коэффициенте корреляции частотных оценок вероятностей s- и $(s + 1)$-грамм.

Теорема 4. *При истинной гипотезе H_* для коэффициента корреляции* $Corr_*\left\{\hat{p}_i(s), \hat{p}_k(s+1)\right\} = \dfrac{\mathrm{cov}_*\left\{\hat{p}_i(s), \hat{p}_k(s+1)\right\}}{\sqrt{D_*\left\{\hat{p}_i(s)\right\} D_*\left\{\hat{p}_k(s+1)\right\}}}$ *частотных оценок вероятностей произвольной пары s- и $(s + 1)$-грамм* $(i, k), i = 0, \ldots, 2^s - 1, k = 0, \ldots, 2^{s+1} - 1$, *справедлива двусторонняя оценка*

$$-2\sqrt{\frac{s}{(s+1)\left(2^s-1\right)\left(2^{s+1}-1\right)}} \le Corr_*\left\{\hat{p}_i(s), \hat{p}_k(s+1)\right\} \le \frac{2^{s+2} - 2s - 4}{\sqrt{s(s+1)\left(2^s-1\right)\left(2^{s+1}-1\right)}}.$$

На рисунке 1 представлена зависимость верхней и нижней границы коэффициента корреляции частотных оценок вероятностей s- и $(s + 1)$-грамм от s. Из рисунка видно, что модуль коэффициента корреляции стремится к 0 с ростом s, причём нижняя граница приближается к нулю экспоненциально быстро. Следовательно, зависимость между оценками энтропии $\hat{h}_s$ и $\hat{h}_s$ по s- и $(s + 1)$-граммам также будет слабой, что позволяет выносить решение о качестве генератора по его энтропийному профилю, пренебрегая этой зависимостью.

На рисунке 2 представлен энтропийный профиль Реньи выходной двоичной последовательности физического генератора [6] длиной $T = 125 \cdot 2^{25}$ бит. На рисунке 3 представлен энтропийный профиль Тсаллиса выходной последовательности программного самосжимающего генератора на основе линейного регистра сдвига с многочленом $x^{24} + x^{11} + x^5 + x^2 + 1$ при фиксированном значении $\lambda = 2$ для $r = 2$ на уровне значимости $\alpha = 0.05$.

Как видно из рисунков 2, 3, для физического генератора гипотеза H_* принимается, для самосжимающего – отклоняется.

В настоящее время в НИИ ППМИ ведётся разработка программного комплекса энтропийного анализа выходных последовательностей криптографических генераторов, который позволит автоматизировать процесс принятия решений и визуализации энтропийных профилей последовательностей.

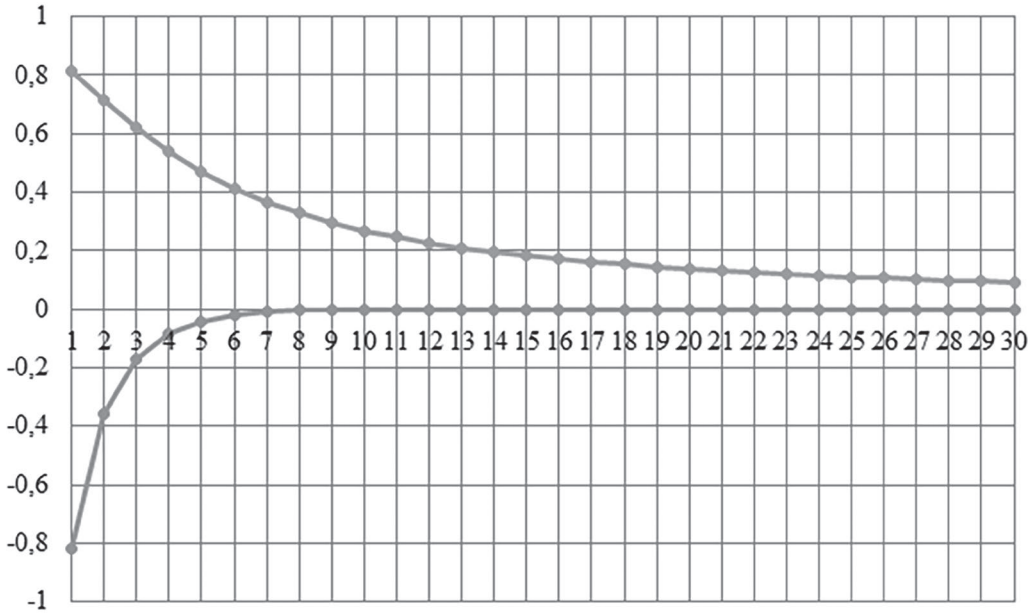


Рисунок 1. Границы коэффициента корреляции частотных оценок

Рисунок 2. Энтропийный профиль Реньи физического генератора

Рисунок 3. Энтропийный профиль Тсаллиса самосжимающего генератора

Список литературы

1. Криптология / Ю. С. Харин [и др.]. – Минск: БГУ, 2013. – 512 с.
2. Харин, Ю. С. Энтропийный анализ криптографических генераторов случайных и псевдослучайных последовательностей / Ю. С. Харин, В. Ю. Палуха // Веснік сувязі. – 2017. – № 6 (146). – С. 40–43.
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. *Acharya, J.* Estimating Renyi Entropy of Discrete Distributions / J. Acharya, [et al.] – IEEE Transactions on Information Theory. – Vol. 63. – No. 1, 2017. – P. 38–56.
5. *Riordan, J.* Moment recurrence relations for binomial, Poisson and hypergeometric frequency distributions / J. Riordan // Annals of Mathematical Statistics. – 1937. – Vol. 8, № 2. – P. 103–111.
6. 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.

УДК 004.056.5

АНАЛИЗ СТОЙКОСТИ КОМБИНИРОВАННОГО МЕТОДА ФОРМИРОВАНИЯ КРИПТОГРАФИЧЕСКОГО КЛЮЧА С СЕКРЕТНОЙ МОДИФИКАЦИЕЙ РЕЗУЛЬТАТОВ СИНХРОНИЗАЦИИ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

М.Л.РАДЮКЕВИЧ

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

Введение. Использование синхронизируемых искусственных нейронных сетей (СИНС) для формирования общего криптографического ключа предложено В. Кантером, И. Кинцелем и описано в [1-5]. В работах [6-8] предложены методы повышения конфиденциальности формируемого общего секрета и уменьшения количества обменов информации по сравнению с технологией Neural key generation. Одним из них является комбинированный метод формирования криптографического ключа с секретной модификацией результатов синхронизации искусственных нейронных сетей (ИНС) (далее – комбинированный метод с секретной модификацией). Предлагается рассмотреть анализ стойкости данного метода.

Комбинированный метод с секретной модификацией**.** Комбинированный метод с секретной модификацией состоит из следующих шагов:

1. Задание входных параметров СИНС: n – количество входов каждого персептрона; K – количество персептронов; ±L – интервал возможных значений весовых коэффициентов персептронов; r – количество строк для функции свертки; $d_{ус}$ – количество тактов синхронизации; V – количество инвертируемых бит;

2. Синхронизация ИНС [9] абонентов А и В до достижения d_{yc}. Данный шаг повторяется r раз. На выходе данного шага получаем бинарные последовательности (БП) $S_r^A(d_{\text{ус}})$ и $S_r^B(d_{\text{ус}})$.
3. Выполнение функции свертки (сложение по модулю 2) r БП, полученных на шаге 2;
4. Внесение некоторых изменений в бинарную последовательность $S_r^A(d_{\text{ус}})$ абонентом А и в $S_r^B(d_{\text{ус}})$ абонентом В, инвертировав случайным образом независимо друг от друга V бит.
5. Устранение несовпадений [10] 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, -тый бит А и В соответственно. Абоненты А и В сообщают четности пар друг другу по открытому каналу связи и каждый сравнивает четности соответствующих пар C_j^A с C_j^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.

Возможные атаки. Возможные атаки строятся на базе отложенного перебора [11]. Полным отложенным перебором назовем атаку, заключающуюся в запоминании значений $\vec{x}(t)$ – случайного входного вектора, $Z^{A/B}(t)$ – выходы сетей, где t = 1, 2, 3, …, $d_{\text{ус}}$, имеющих место при синхронизации сетей A и B, и многократном повторении синхронизаций сети E с различными начальными значениями ВК с одними и теми же сетями и , на входы которых подается записанный $\vec{x}(t)$, а выходы равны $Z^{A/B}(t)$. Критерием успешного перебора является совпадение C_j^A с C_j^B по окончании синхронизации, как промежуточный успех, и полное совпадение процесса отсеивания несовпадающих битов в $S_r^A(d_{\text{ус}})$ и $S_r^B(d_{\text{ус}})$ на пятом шаге метода. Окончательным подтверждением успеха атаки является совпадения секрета, сформированного A и B с секретом E, фиксируемое по одному из критериев [6]. Очевидно, что вероятность успеха рассматриваемой атаки равна $P_{AE,r}(d_{yc})$. Действительно, если для некоторого набора начальных значений ВК сети E окажется, что она достигла полного синхронизма с сетью A до наступления такта d_{yc}, то в дальнейшем будет выполнено $S_r^A(d_{\text{ус}}) = S_r^B(d_{\text{ус}})$ и $C_j^A = C_j^B$, что означает успех атаки.

Известно, что количество возможных комбинаций значений ВК ИНС Е равно $M = (2L+1)^{K*n}$. При предлагаемых значениях L, K, n осуществить полный перебор значений технически сложно в ближайшем будущем. Однако, как показано в [10] при отложенном переборе абоненту E совершенно необязательно угадать истинное начальное значение вектора весовых коэффициентов ИНС A или B, т.к. существует достаточно большое множество начальных значений вектора весовых коэффициентов ИНС E, движение из которых при благоприятных траекториях $\vec{x}(t)$ позволяет обеспечить пересечение траекторий движения $S_r^A(t)$ и $S_r^B(t)$, в смысле равенства всех их элементов. После такого пересечения траектории движения $S_r^A(d)$ и $S_r^B(d)$ совпадают при всех последующих тактах синхронизации. В результате обязательно наступит $S_r^A(d_{\text{ус}}) = S_r^B(d_{\text{ус}})$. Таким образом, если при классическом полном переборе значений успех атаки наступает при единственно правильном наборе ВК ИНС E, то в атаке отложенным перебором успех атаки наступает при всех наборах для

которых ВК ИНС E пересеклись с ВК ИНС A на участке от $t = 0$ до $t = d_{yc}$. Этот эффект качественно поясняется на рисунке 1.

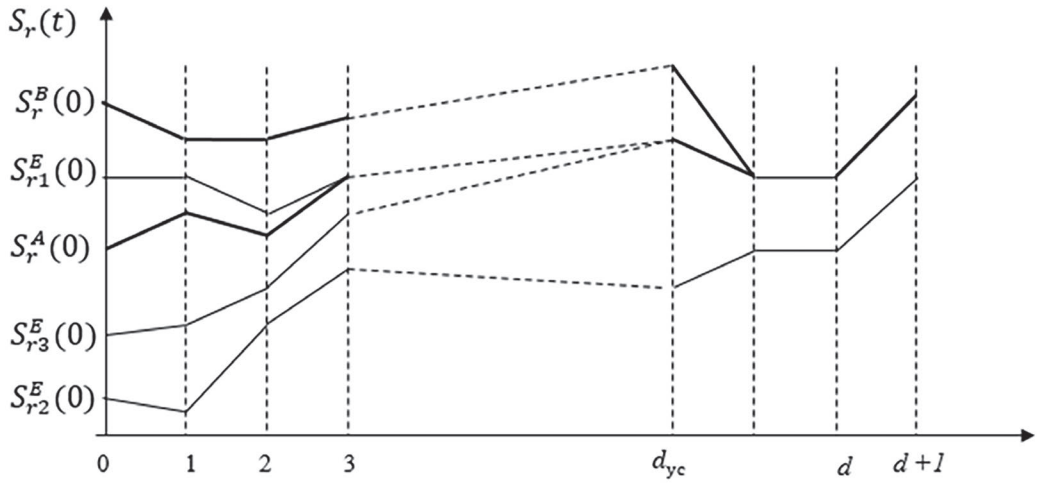


Рисунок 1. Условное графическое отображение синхронизаций

На этом рисунке показаны условные траектории изменения векторов весовых коэффициентов сетей A, B в процессе синхронизации. Сеть E представлена тремя типами траекторий.

Для траекторий типа $S_{r1}^E(t)$, пересекающихся с $S_r^A(t)$ на участке от $t = 0$ до $t = d_{yc}$ обязательно выполняется $S_r^A(d_{yc}) = S_r^B(d_{yc})$, что обнаруживается E по равенству объявленных значений C_j^E, C_j^A и полному совпадению процесса отсеивания несовпадающих битов между $S_r^A(d_{yc})$, $S_r^B(d_{yc})$ и $S_r^A(d_{yc})$, $S_r^E(d_{yc})$, при этом вероятность успеха такой атаки равна $P_{AR,r}(d_{yc})$.

Траектории типа $S_{r2}^E(t)$, не пересекаются с $S_r^A(t)$ на участке от $t = 0$ до $t = d_{yc}$. Траектории этого типа составляют большинство, их вероятность равна $1 - P_{AR,r}(d_{yc})$.

Траектория типа $S_{r3}^E(t)$ в процессе синхронизации пересеклась с $S_r^A(t)$ в точке $t = d_{yc}$. Вероятность получения такой траектории близка к вероятности независимого перебора всех возможных значений $S_r^A(d_{yc})$, которая равна $(2L+1)^{-K*n}$.

Таким образом, несмотря на то, что за счет выбора минимально возможного значения d_{yc} и усложнения процесса синхронизации за счет увеличения r, вероятность успеха атаки отложенного перебора намного больше, чем $(2L+1)^{-K*n}$. Этот факт может быть объяснен тем, что в одном случае успех атаки обусловлен тем, что достаточно найти хотя бы одну траекторию $S_r^E(t)$, пересекающуюся с траекторией $S_r^A(t)$ на интервале $[0, d_{yc}]$, а во втором случае нужно найти единственную траекторию $S_r^E(t)$, проходящую через точку $S_r^A(d_{yc})$.

Однако, за счет инвертирования случайным образом абонентами A и B независимо друг от друга некоторого количества битов на четвертом шаге метода значительно повышается криптостойкость по отношению к данной атаке. Этот эффект показан на рисунке 2.

Действительно, внесение случайного секретного изменения некоторых битов в $S_r^A(d_{yc})$ и $S_r^B(d_{yc})$ превращает атаку отложенный перебор из поиска траекторий $S_r^E(t)$, пересекающихся с траекторией $S_r^E(t)$, в поиск траектории $S_r^E(d_{yc})$, проходящей через точку $\hat{S}_r^A(d_{yc})$, где $\hat{S}_r^A(d_{yc})$ – случайно модифицированная точка $S_r^A(d_{yc})$.

Оценим вероятность успеха атаки. Так как при относительно небольших выбранных значениях d_{yc} корреляция между $S_r^E(t)$ и $S_r^E(t)$ довольно слабая (обозначим ее n_{EA}^{cb}/b) и составляет $\approx 0{,}5$, то различные траектории $S_r^E(t)$ можно считать независимыми между собой,

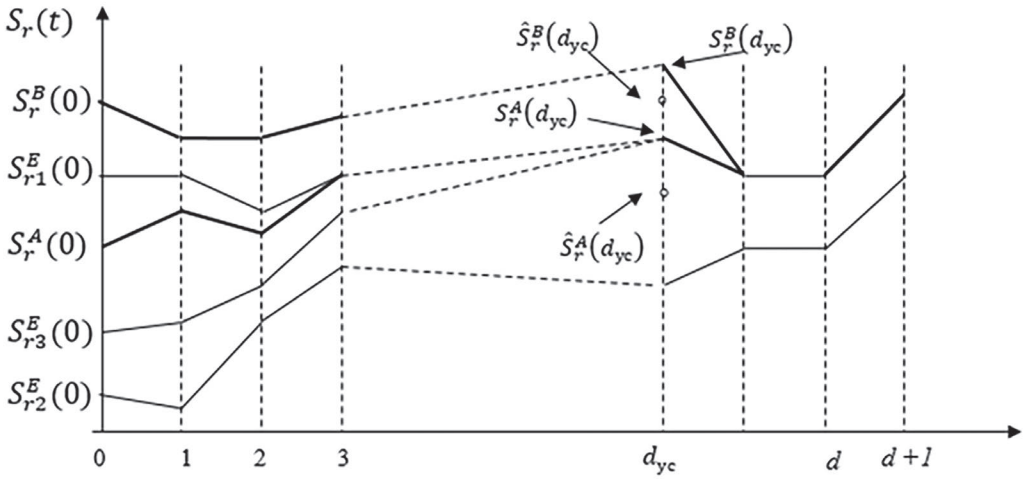


Рисунок 2. Модификация результата синхронизации

а перебор в данном случае эквивалентен поиску такой единственной совокупности начальных значений ВК своей сети, которые приведут ИНС E к попаданию в точку $\hat{S}_r^A(d_{yc})$. Следовательно, вероятность успеха такого перебора близка к величине $(2L)^{-K*n}$. Например, для $L = 8$, $K = 3$, $n = 1000$ имеем $P_{op1} = 2.3*10^{-3612}$.

Второй вариант атаки заключается в том, что абонент E, перебирая начальные значения ВК своих сетей, доводит каждую синхронизацию $S_r^E(t)$ до $t = d_{yc}$, затем модифицирует полученную БП по аналогии с модификацией, проделанной А и В, перебирая все возможные варианты инвертирования битов. Если для какого-то варианта окажется, что $\hat{C}_i^E = \hat{C}_i^A$ и процесс удаления несовпадающих битов $\hat{S}_r^E(d_{yc})$ полностью совпал с процессом удаления несовпадающих битов в $\hat{S}_r^A(d_{yc})$, то атака является успешной. Оценим вероятность успеха этой атаки, обозначив ее через P_{op2}.

Атака будет успешной, если после некоторой синхронизации ИНС Е с ИНС А и последующего перебора инвертированных битов в $S_r^E(d_{yc})$ окажется, что $\hat{S}_r^A(d_{yc}) = \hat{S}_r^E(d_{yc})$. Обозначим это событие через U. Событие U произойдёт, если при синхронизации ИНС E и A произойдёт событие $S_r^A(d_{yc}) = S_r^E(d_{yc})$, обозначим его и при переборе некого числа битов ϑ в $S_r^E(d_{yc})$ будет найдена комбинация битов, инвертированных в $S_r^A(d_{yc})$ (событие B). Кроме того, событие U будет иметь место, если произойдет событие и будет найдена комбинация битов несовпадающих в $S_r^E(d_{yc})$ и $\hat{S}_r^A(d_{yc})$, возникшая за счет различия начальных значений ВК ИНС E и A и последующего инвертирования некого числа битов в $S_r^A(d_{yc})$, т.е. события С.

С учетом введенных обозначений имеем

$$P_{op2}(U) - P(A)P(B) + P(\overline{A})P(C). \qquad (1)$$

Определим составляющие (1):

$$P(A) = P(S_r^E(d_{yc}) = S_r^A(d_{yc})) = P_{AE,r}(d_{yc}).$$

Для первого варианта инвертирования имеем

$$P(B) = (C_b^V)^{-1},$$

где b длина БП $S_r^E(d_{yc})$ и $S_r^A(d_{yc})$ в битах.

$$P(\overline{A}) = 1 - P(A) = 1 - P_{AE,r}(d_{yc});$$

$$P(C) \approx (\sum_{v=\frac{b}{2}-V}^{\frac{b}{2}+V} C_b^v)^{-1}.$$

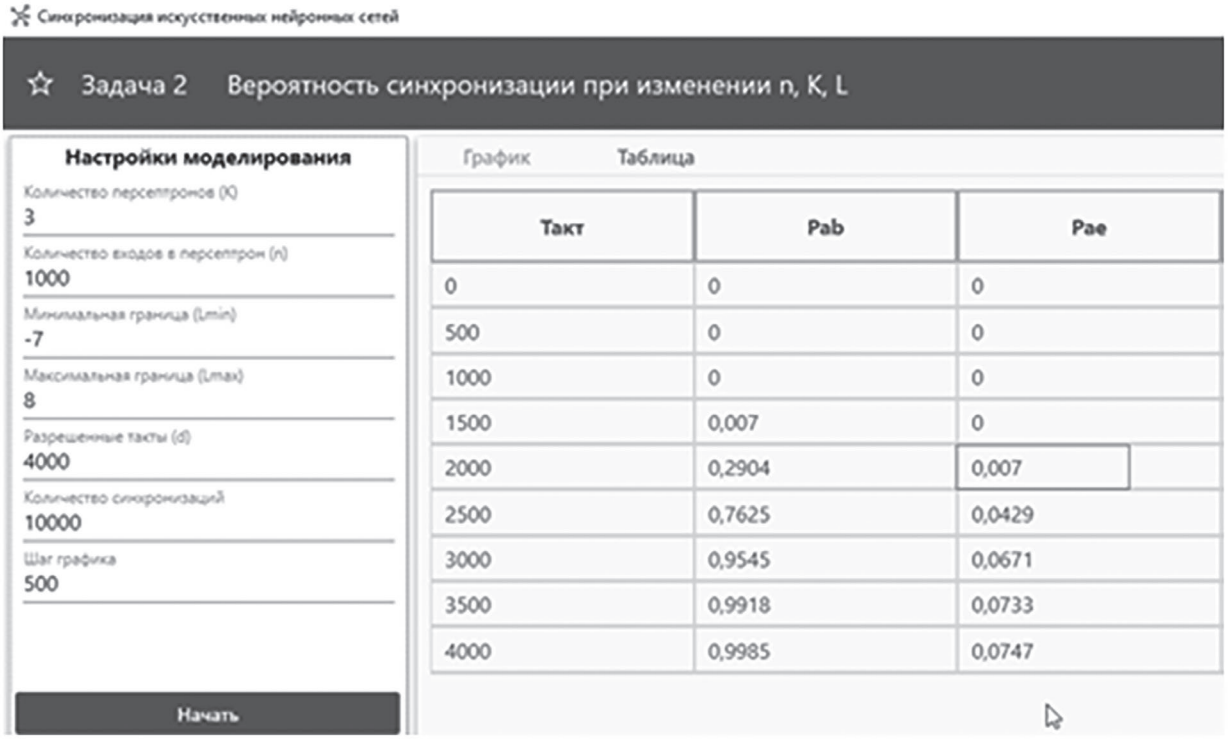


Рисунок 3. Вероятности синхронизаций сетей A, B и E

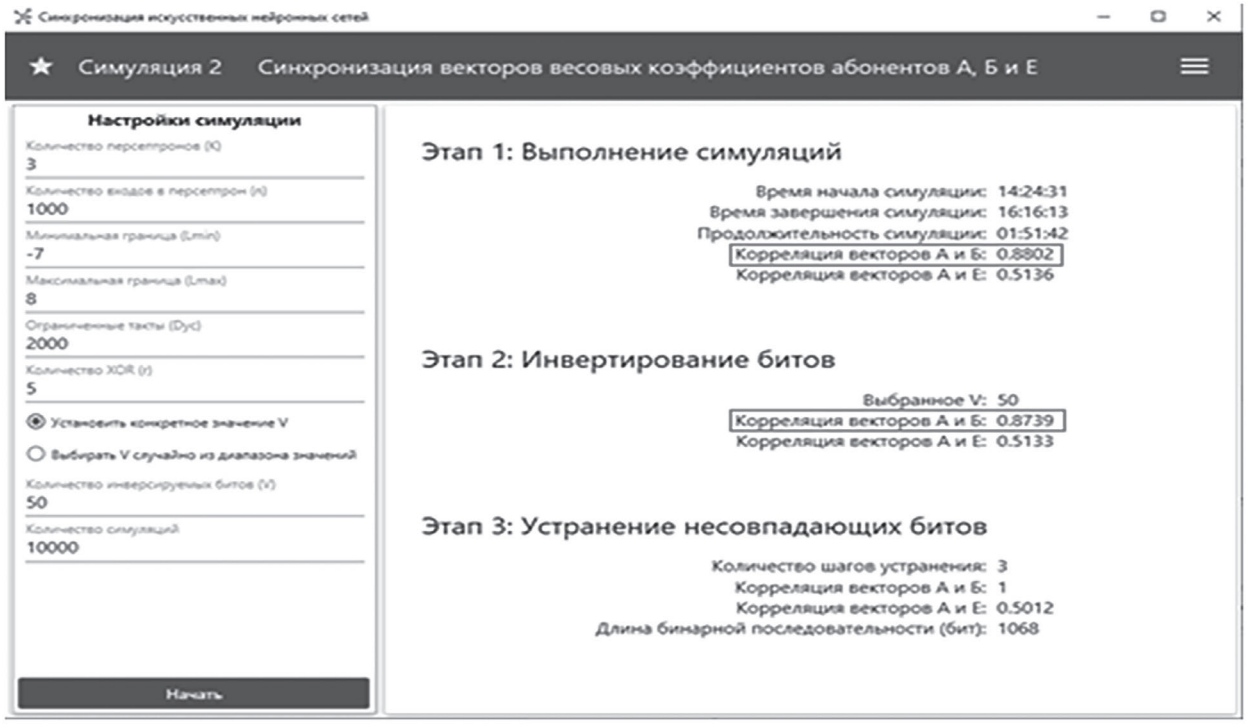


Рисунок 4. Влияние V на корреляцию векторов A и B

Пределы перебора инвертированных битов в $P(C)$ определены приближенно, исходя из следующих соображений. Известно, что для БП слабо коррелированных между собой, а $S_r^E(d_{\text{ус}})$ и $S_r^A(d_{\text{ус}})$ являются таковыми математическое ожидание числа несовпадающих битов

равно $b/2$. Дополнительное инвертирование некого числа битов может лишь незначительно увеличить или уменьшить число несовпадающих битов. Окончательно имеем

$$P_{op2} = P(U) \approx P_{AE,r}(d_{yc})(C_b^V)^{-1} + (1 + P_{AE,r}(d_{yc}))(\sum_{v=\frac{b}{2}-V}^{\frac{b}{2}+V} C_b^v)^{-1} \quad (2)$$

Так как $(\sum_{v=\frac{b}{2}-V}^{\frac{b}{2}+V} C_b^v)^{-1} \ll (C_b^V)^{-1}$, то вторым слагаемым в (2) можно пренебречь

$$P_{op2} = P(U) \approx P_{AE,r}(d_{yc})(C_b^V)^{-1} \quad (3)$$

Проиллюстрируем масштаб перебора. Зададимся начальными параметрами $K = 3$, $n = 1000$, $L_1 = -7$, $L_2 = -8$, $r = 5$, $d_{yc} = 2000$, $b = 12000$, $V = 50$. Проведем моделирование для получения значений $P_{AE,r}(d_{yc})$ и n_{EA}^{cb}/b. Объем моделирования 10^4. Результаты моделирования представлены на рисунках 3 и 4.

Рисунок 3 отображает результаты моделирования $P_{AE}(d_{yc})$. Значения $P_{AE,r}(d_{yc})$ высчитывается по формуле $P_{AE,r} = (P_{AE})^r$. Для $d_{yc} = 2000$ и получаем $P_{AE,r}(d_{yc}) = (0.007)^5 = 1.68*10^{-11}$.

Из результатов моделирования на рисунке 4 нас интересуют значения корреляции векторов A и B до инвертирования случайных битов и после. В результате моделирования мы получили до инвертирования $\overline{n}_{AB}^{cb}/b = 0.8802$, после инвертирования $\overline{n}_{AB}^{cb}/b = 0.8739$.

Подставляя полученные значения и значение $(C_b^V)^{-1} \approx 2.7*10^{-139}$ в формулу (3) получаем $P_{op2} = 1.68*10^{-11}*2.7*10^{-139} \approx 4.54*10^{-150}$.

Следует отметить, что за счет инвертирования 50 битов в $\hat{S}_r^A(d_{yc})$ и $\hat{S}_r^B(d_{yc})$ общее количество совпадающих битов в них может уменьшиться максимально на 100 (все инвертированные биты в $S_r^A(d_{yc})$ не совпали с инвертированными битами в $S_r^B(d_{yc})$), минимально на 0 (все инвертированные биты в $S_r^A(d_{yc})$ совпали с инвертированными битами в $S_r^B(d_{yc})$). Таким образом относительное среднее количество совпадающих битов в $S_r^A(d_{yc})$ и $S_r^B(d_{yc})$ может сократиться с $\overline{n}_{AB}^{cb}/b = 0.8802$ до $\overline{n}_{AB}^{cb}/b = 0.8739$, что практически не вызовет увеличения числа итераций при устранении несовпадающих битов.

Таким образом, комбинированный метод с секретной модификацией результата синхронизации существенно повышает криптостойкость сформированного ключа.

Заключение. Рассмотренные атаки на комбинированный метод формирования криптографического ключа с секретной модификацией результатов синхронизации искусственных нейронных сетей не представляют угрозы в ближайшем будущем, так как данный метод обеспечивает высокую его криптостойкость, соизмеримую с криптостойкостью современных алгоритмов симметричного шифрования, при относительно простой реализации.

Список литературы

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. Ruttor, A. Dynamics of neural cryptography / A. Ruttor, I. Kanter, and W. Kinzel // Phys. Rev. E, 75(5):056104, 2007.

5. Плонковски, М. Криптографическое преобразование информации на основе нейросетевых технологии / М. Плонковски, П. П. Урбанович // Труды БГТУ. Сер. VI. Физико-математические науки и информатика; под ред. И. М. Жарского. – Минск: БГТУ, 2005.
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. Комбинированный метод формирования криптографического ключа с секретной модификацией результатов синхронизации искусственных нейронных сетей //Системный анализ и прикладная информатика. – 2021. – № 3. – С. 51–58.
9. 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.
10. Пивоваров В.Л., Голиков В.Ф. Способ формирования криптографического ключа для слабо совпадающих бинарных последовательностей. Информатика, № 3(51), 2016. Стр. 31-37.
11. Голиков, В. Ф. Атака на синхронизируемые исскуственные нейронные сети, формирующие общий секрет, методом отложенного перебора / В. Ф. Голиков, А. Ю. Ксеневич // Доклады БГУИР. – 2017. – № 8. – С. 48–53.

АКТУАЛЬНЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЮЗНОГО ГОСУДАРСТВА

УДК 608.2

К ВОПРОСУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИМПОРТОЗАМЕЩЕНИЯ ЗАУРБЕЖНЫХ ИНТЕГРАЛЬНЫХ СХЕМ ИЗМЕРЕНИЯ МОЩНОСТИ

А.В. КУШНЕРОВ, И.В. МУРИНОВ
Научно-производственное республиканское унитарное предприятие
«Научно-исследовательский институт технической защиты информации»
г.Минск, ул.Первомайская, д.26, к.2, 246034, Республика Беларусь

Получение достоверной информации об измеряемой мощности является одной из основных задач, решаемых при создании информационно-измерительных преобразователей. Особенность построения таких устройств состоит в том, что для их создания должны применяться электронные компоненты, реализующие, во-первых, получение корректной информации о мощности путём перемножения с требуемой точностью аналоговых сигналов, пропорциональных току и напряжению контролируемой электрической сети, и, во-вторых, обеспечение информационной безопасности для надёжной защиты информации, обмен которой эти устройства обычно осуществляют с центром учёта энергии.

Среди современных электронных компонентов (включая также демонстрационные и отладочные комплекты разработчика), решающих указанную задачу, наиболее широкую известность, распространение и применение получили интегральные микросхемы, производимые лидерами электронной промышленности стран Европы, Азии и США, занимающими значительный процент мирового рынка [1].

К настоящему времени по разным причинам во многом нарушены и продолжают ухудшаться условия, по которым страны, не обладавшие собственной и развитой в полной мере электронной полупроводниковой промышленностью или отставшие в этой отрасли производства от лучших представителей мирового уровня, имели до недавней поры относительно свободный доступ к результатам научно-производственной деятельности передовых стран в сфере высоких технологий. Также на первый план выдвигаются вопросы информационной безопасности и импортозамещения в области производства электронных компонентов.

В складывающейся обстановке в Республике Беларусь действует принятая правительством «Государственная программа «Цифровое развитие Беларуси» на 2021–2025 годы» (постановление Совета министров Республики Беларусь от 2 февраля 2021 г. №66), а в России – «Стратегия развития электронной промышленности Российской Федерации на период до 2030 года» (распоряжение Правительства РФ от 17 января 2020 г. № 20-р), согласно которым, помимо прочих задач, должны решаться вопросы развития сегмента полупроводников и собственной электронной промышленности. Основной проблемой при этом является трудность осуществления полной локализации производства микроэлектроники на базе современного технологического процесса (менее 90 нанометров), поскольку главным препятствием для достижения этой цели является отсутствие собственного оборудования (в том числе машин фотолитографии) для печати микросхем, которое производят

нидерландская ASML, японские Canon и Nikon, а США, являясь владельцами патентов на отдельные технологические составляющие, блокируют их отгрузку в Россию и Республику Беларусь [2]. Создание же собственных машин фотолитографии – долгосрочный процесс, требующий значительных трудовых и финансовых ресурсов.

Преодоление проблем на пути развития собственного производства микросхем также связано с основополагающей особенностью создания чипов – двойственностью этого процесса, которая состоит в том, что для их изготовления также должны решаться задачи по их разработке. Поэтому, для успешной реализации планов по созданию собственного производства микросхем, это производство должно быть наполнено технологиями изготовления чипов конкретного назначения, подобранными для воссоздания в них востребованных принципов, функций и алгоритмов обработки сигналов, и гарантирующими отсутствие недокументированных вредоносных возможностей.

С учётом вышеизложенного, в качестве одного из вариантов построения преобразователя мощности для его реализации в интегральном исполнении предлагается высокоточный быстродействующий импульсный перемножитель аналоговых сигналов [3-5], предназначенный, в том числе, для использования в счётчиках энергии. Его принцип действия состоит в преобразовании одного из двух аналоговых сигналов в скважность, длительности которой (дискретные отсчёты) управляют работой электронных ключей аналогового модулятора, на вход которого поступает второй аналоговый сигнал. При этом среднее значение выходного сигнала модулятора, формируемое сглаживающим фильтром, пропорционально перемножению этих двух сигналов.

В современных условиях развития комплексной автоматизации энергосистем, а также увеличения мощностей электростанций и потребителей электроэнергии, потребность в высокоточном измерении энергии и защиты передаваемых данных только возрастает, и в настоящее время актуальным становится улучшение класса точности до 0,2-0,5 (на сегодня выпускаемые промышленностью счётчики электрической энергии имеют класс точности 1,5-4,0). Поскольку погрешность счётчиков в основном определяется погрешностью преобразователя мощности, выполняющего перемножение по мгновенным значениям сигналов, пропорциональных току и напряжению, то для построения счётчиков энергии повышенного класса точности необходимы преобразователи мощности, которые могут обеспечить погрешность 0,05-0,2%.

Разработка высокоточного преобразователя для таких счётчиков должна учитывать то, что счётчик, выполняя интегрирование мгновенной мощности за время измерения, накапливает погрешность преобразователя мощности. С учётом этого качество преобразователя мощности необходимо определять не по приведённой, а по относительной погрешности, которая позволяет правильно оценить допустимую погрешность во всём диапазоне изменения измеряемой величины. Из этого следует, что, поскольку методическую погрешность преобразователя во многом определяет реализуемый схемой метод перемножения сигналов, то выбирать следует метод, у которого эта погрешность минимальна.

Высокую точность перемножения можно обеспечить, если представить сомножители в цифровой форме. Однако, необходимые для этих целей быстродействующие аналого-цифровые преобразователи имеют большую стоимость, что препятствует широкому внедрению устройств на их основе. Реализация аналоговых способов перемножения сигналов обходится дешевле цифрового и используется более широко, например, серийно производимые измерительные преобразователи (Е851, Е856-Е858, Е842 и Е848-М1) с пределом допускае-

мой приведённой основной погрешности 0,5%, в которых измерительный преобразователь мгновенной мощности является перемножителем импульсного типа.

Таким образом, представленный здесь вариант высокоточного быстродействующего импульсного перемножителя обладает необходимыми достоинствами – даёт правильный результат по небольшому числу (от трёх) дискретных отсчётов (в отличие от микропроцессорных с АЦП) и имеет высокую по относительной погрешности точность (в отличие от перемножителей аналоговых сигналов в интегральном исполнении серии ПС). При создании микросхем, несущих в своей структуре такой перемножитель, они могут быть использованы при реализации преобразователей мгновенной мощности высокой точности и быстродействия, применяемые при построении необходимых устройств, датчиков направления мощности и дешёвых АЦП. Собственная, а потому контролируемая, разработка и производство чипов такого типа также оправданы тем, что обеспечат возможность их использования в критически важных областях народного хозяйства, решая ещё одну важную задачу – гарантированная защита чипов от наличия вредоносных недокументированных возможностей, которые могут быть в микросхемах иностранного производства.

Список литературы

1. Полупроводники. Мировой рынок [электронный ресурс] – (URL: https://www.tadviser.ru/index.php/Статья:Полупроводники_(мировой_рынок), дата обращения – 25.04.2022).
2. Ю.Борта, А.Прикладова – Чипам нужно спешить на помощь. Сможет ли РФ производить свою электронику? // Аргументы и факты (URL: https://aif.ru/money/market/ chipam_nuzhno_speshit_na_pomoshch_smozhet_li_rf_proizvodit_svoyu_elektroniku, дата обращения 03.05.2022).
3. И.В.Муринов – Быстродействующий импульсный перемножитель аналоговых сигналов. // Материалы 54-й МНТК БГПА, г.Минск, 2000, часть 3, с.72.
4. Е.Г.Абаринов – Быстродействующий преобразователь активной мощности. // Энергосбережение. Электроснабжение. Автоматизация: материалы МНТК – г.Гомель, Учреждение образования ГГТУ им.П.О.Сухого, 2001, с.98-99.
5. Е.Г.Абаринов, И.В.Муринов – Выбор и расчёт многозвенных сглаживающих фильтров информационных преобразователей среднего значения по заданному быстродействию. // «Измерительная техника», М.: Изд-во стандартов, 1999, №12.

УДК 034.096

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ВОПРОСЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Т.В. РАДЫНО

Республиканское общественное объединение
«Белорусская научно-промышленная ассоциация»,
г. Минск, Республика Беларусь

В ноябре 2021 года вступил в силу Закон Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» (далее – Закон). Практика его применения обнаружила

много неясностей, несмотря на то, что создание Закона осуществлялось с учетом лучшего мирового опыта.

Одна из новаций Закона – это закрепление понятия «персональные данные». Тем не менее, уже сейчас очевидно, что данное в Законе определение не дает возможности однозначно очертить границы, в рамках которых существует перечень относимых к таким данным сведений. На практике уже имеет место расширенное (с учетом мировой практики) толкование названного понятия.

Анализ норм Закона очерчивает направления, которые требуют первоочередной дополнительной проработки практики его применения участниками гражданских правоотношений.

Порядок обращения с персональными данными в конкретной организации должен быть регламентирован локальными правовыми актами. В первую очередь, необходимо в политике конфиденциальности либо в отдельных документах, регламентировать и разъяснить порядок обработки персональных данных. Далее, необходимо обучить сотрудников правилам обработки персональных данных, определить лиц, ответственных за обработку персональных данных, в необходимых случаях – создать отдел, специализирующийся на работе с персональными данными. При этом необходимо учитывать, что доступ к персональным данным должен иметь объективно ограниченный круг лиц.

Организация защиты персональных данных подразумевает также, что необходимо дополнительно закупить специальное оборудование. Так, если субъект хозяйствования планирует пользоваться сторонними сервисами (например, Google ads, платежные сервисы) либо передавать персональные данные для маркетинговых исследований, а также пользоваться услугами уполномоченных лиц (государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, которые в соответствии с актом законодательства, решением государственного органа являются операторами либо на основании договора с оператором осуществляют обработку персональных данных от имени оператора или в его интересах), следует заключить договор с такими уполномоченными лицами (пункт 1 статьи 7 Закона).

Напомним, что в Законе предусмотрено 3 (три) вида согласия на обработку персональных данных: письменная форма, электронный документ или иная электронная форма. Создание электронных форм для получения согласия в онлайн-формате – обязательное условие функционирования торговли по образцам, которой является интернет-магазин.

Особо можно выделить организацию работы с персональными данными представителей ритейла, у которых существуют бонусные программы и программы лояльности. Представителям данной сферы необходимо получить согласия всех субъектов персональных данных на обработку таких данных, иначе бонусные программы и программы лояльности – не что иное, как нарушение Закона, поскольку единственным легитимным основанием для обработки персональных данных клиентов – участников бонусных программ является согласие субъекта персональных данных (часть 1 пункта 3 статьи 4 Закона).

Не следует также забывать о том, что до получения согласия субъекта персональных данных оператор (лицо, которое обрабатывает персональные данные) в письменной либо электронной форме, соответствующей форме выражения такого согласия, обязан представить субъекту персональных данных предусмотренную в Законе информацию (пункт 5 статьи 5 Закона).

Отметим, что получение согласия – это завершающий этап. До момента получения согласия субъекта персональных данных оператор обязан простым и ясным языком разъяснить

субъекту персональных данных его права, связанные с обработкой персональных данных, механизм реализации таких прав, а также последствия дачи согласия субъекта персональных данных или отказа в даче такого согласия. Эта информация должна быть представлена оператором субъекту персональных данных в письменной либо электронной форме, что важно – 1. соответствующей форме выражения его согласия, 2. отдельно от иной представляемой ему информации (статья 5 Закона).

Термин «отдельно» – это еще один термин, который вызывает разночтения на практике, поскольку на данный момент Закон не разъясняет, как его понимать.

Так, не совсем ясно, достаточно ли выделения такой информации иным шрифтом, абзацным отступом либо такая информация должна содержаться в самостоятельном документе. Вместе с тем нарушение прав физического лица, связанных с обработкой персональных данных, грозит штрафом до 50 базовых величин.

Отдельно следует отметить требования к согласию субъекта персональных данных, как «свободному, однозначному, информированному выражению его воли, посредством которого он разрешает обработку своих персональных данных».

Классическое свободно выраженное согласие – это то, от которого субъект может отказаться, но при этом удовлетворить свои потребности, получив полный объем услуг. Например, мировая практика идет по пути использования интернет-порталов пользователями с возможностью использования настраиваемых параметров cookies.

Однозначность выражения воли, например, может подразумевать, что при использовании интернет-ресурсов следует считать нарушением Закона и, соответственно, нарушением порядка обработки персональных данных пользователей, формулировки вроде «оставаясь на сайте, вы даете согласие на обработку ваших персональных данных».

Выражение воли должно осуществляться на основе информированности, когда субъект персональных данных обладает всеми необходимыми и достаточными сведениями, предусмотренными Законом, четко знает, кто, как долго и для каких целей будет использовать его персональные данные. Следовательно, операторам следует понимать, что этот принцип налагает на них обязанность четко определить категории персональных данных, определить цели их обработки и лиц, имеющих к таким данным доступ.

Отдельные выводы очевидны уже сегодня: при представлении информации субъекту персональных данных, при получении согласия на обработку персональных данных должны отсутствовать нечеткие, допускающие неоднозначное толкование формулировки. Идеально было бы, чтобы при даче письменного согласия на обработку персональных данных субъект **собственноручно** писал, что «он дает согласие свободно, ему разъяснены все права, возможности управления своими персональными данными и субъект понимает, в каком порядке, кем и в каких целях они будут использованы».

Довольно много споров вызывает норма части 1 пункта 6 статьи 5 Закона, которая предполагает, что субъект персональных данных при даче своего согласия оператору указывает свои фамилию, собственное имя, отчество (если таковое имеется), дату рождения, идентификационный номер, а в случае отсутствия такого номера – номер документа, удостоверяющего его личность. Бытует мнение, что операторы должны, исходя из построения указанной нормы, получать у клиентов паспортные данные всегда, например, карты лояльности нельзя будет выдавать без получения паспортных данных клиентов.

Системный анализ понятия «обработка персональных данных», (к которой относится, напомним, ***любое действие*** *или совокупность действий, совершаемые с персональными данными, включая* ***сбор****, систематизацию,* ***хранение****, изменение, использование, обезличи-*

вание, блокирование, распространение, предоставление, удаление персональных данных) и нормы части 2 пункта 6 статьи 5 Закона позволяют говорить о том, что в законодательстве относительно согласия на обработку персональных данных отсутствует императивное требование о предоставлении паспортных данных субъекта, если эти данные нет необходимости получать в конкретной ситуации. Это еще раз подводит нас к обязанности операторов по ясному и четкому определению целей обработки персональных данных, а также видов данных, которые подлежат обработке.

На момент вступления в силу Закона, многие субъекты хозяйствования по роду деятельности уже обладали большими и актуальными базами персональных данных клиентов. Естественно, возник вопрос, как поступать с этими данными. Очевидно, что необходимо получить согласие на обработку ранее полученных персональных данных в соответствии с требованиями Закона. В случае, когда субъект персональных данных не даст согласие на обработку данных либо откажется от обработки персональных данных (например, письменно), следует принять меры к обезличению либо удалению персональных данных.

Таким образом, как бы ни хотелось субъектам хозяйствования использовать персональные данные максимального количества лиц, необходимо учитывать новые возможности, предоставляемые субъектам персональных данных Законом и одновременно новые ограничения, налагаемые на операторов персональных данных (часть 1 пункта 1, пункт 2 статьи 12 Закона).

Также Закон устанавливает ряд требований к информации, которую субъект данных должен указать в таком заявлении (статья 14 Закона).

Указанное приводит нас к выводу о том, что уже сегодня субъектам хозяйствования следует решить ряд организационно-правовых вопросов и, вероятно, приготовиться к дополнительным финансовым и иным издержкам.

Еще один момент, который важно учесть при организации обработки персональных данных, что уполномоченное третье лицо не обязано самостоятельно получать согласие субъекта персональных данных, за это отвечает оператор (статья 7 Закона).

Еще один серьезный вопрос – это трансграничная передача данных. Так, при определенных условиях использование серверов, физически находящихся вне территории Республики Беларусь является трансграничной передачей данных, на которую необходимо получать согласие. Однако, не всегда возможно однозначно определить местонахождение сервера.

Подводя итог, следует отметить, что потребуются максимальные усилия для организации надлежащей защиты персональных данных, обработка персональных данных потребует реализации целого комплекса организационных и правовых мер: подготовки необходимого спектра документов с привлечением юристов, программистов, иных технических специалистов. Необходимо внимательно проанализировать все внутренние производственные процессы в организации, разработать индивидуальный подход к своим внутренним регламентам на основе комплексного внутреннего аудита.

В настоящее время создан уполномоченный орган по защите прав субъектов персональных данных, который проводит разъяснительную работу по законодательству о персональных данных. Таким образом, по мере накопления правоприменительной практики эти и другие вопросы постепенно получат свои пути решения; от того, по какому пути пойдет практика, и какую позицию займет уполномоченный орган по защите прав субъектов персональных данных, будет зависеть перспектива максимально безболезненной реализации положений Закона на практике.

УДК 004.056.53

ПЕРСПЕКТИВЫ РАЗВИТИЯ МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ БЕЛАРУСИ И РОССИИ

Е.Е. БУТРИК ,С.В. СОЛОВЬЕВ, Ю.К. ЯЗОВ
Федеральное автономное учреждение «Государственный научно-исследовательский институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю»,
г. Воронеж, 394020, Российская Федерация

Деятельность по защите информации (ЗИ) в информационных системах (ИС) Беларуси и России сегодня связана с решением широкого круга задач, определяемых содержанием предметной области ЗИ, требованиями государственных регуляторов и касающихся таких аспектов, как:

- обоснование классов (уровней) защищенности ИС;
- выявление уязвимостей в архитектуре, в системном и прикладном программном обеспечении (ПО) ИС;
- выявление и оценка рисков реализации возможных угроз безопасности информации;
- обоснование требований по ЗИ, определение целесообразных путей построения систем защиты информации в составе ИС;
- организация и проведение контроля и оценка защищенности информации, обрабатываемой в ИС по его результатам и др.

Решение этих задач невозможно без соответствующего методического обеспечения. Сегодня в соответствии с существующим представлением о предметной области технической защиты информации в ИС чаще всего рассматривают пять направлений такого обеспечения, включающего математические модели, методики и алгоритмы (рисунок 1):

- прогнозирования новых уязвимостей и угроз безопасности информации в ИС;
- анализа угроз безопасности с оценкой способов и последствий их реализации в ИС;
- ведения национального банка данных угроз безопасности информации;
- обоснования требований по защите информации в ИС, в том числе требований к мерам, средствам и системам ЗИ;
- построения систем ЗИ;
- организации и ведения контроля защищенности информации в ИС и эффективности ЗИ.

Перспективы развития методического обеспечения прогнозирования угроз, ведения банка данных угроз безопасности информации, а также частично экспериментальных исследований возможности реализации угроз рассматривалось на XXVI конференции «Комплексная защита информации» в 2021 г., поэтому далее рассматриваются в основном остальные из указанных направлений развития методического обеспечения.

Характеризуя состояние и перспективы развития методического обеспечения анализа угроз безопасности информации необходимо отметить следующее.

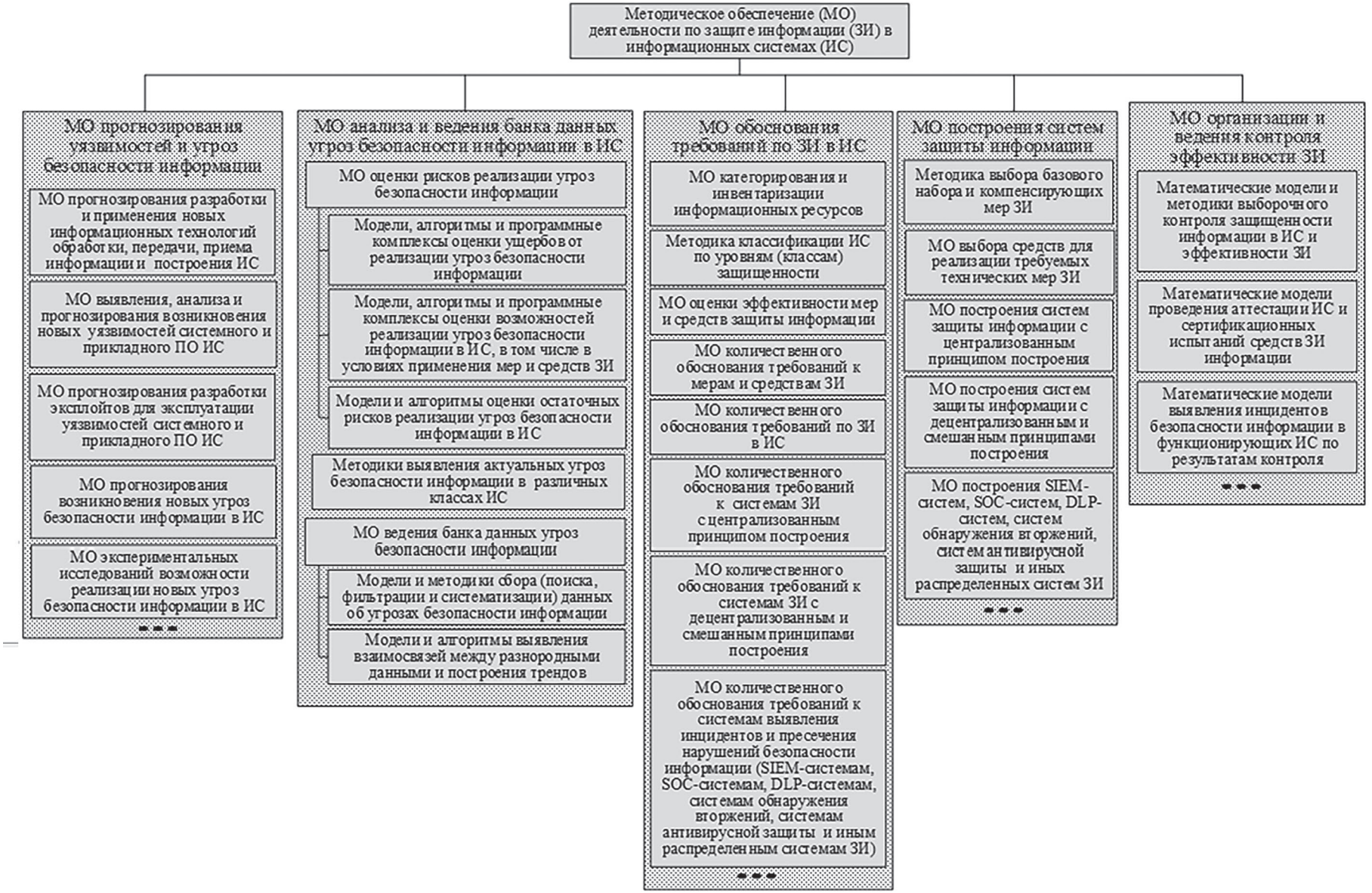


Рисунок 1. Структура методического обеспечения деятельности по технической защите информации в информационных системах

Анализ угроз безопасности информации в ИС связан, прежде всего с оценкой возможностей реализации угроз и ожидаемого ущерба от такой реализации, то есть с оценкой риска реализации угроз, под которым понимается произведение математического ожидания возможного ущерба на вероятность реализации угрозы.

Несмотря на то, что идеи количественной оценки риска реализации угроз безопасности информации появились в той или иной форме уже более 30 лет назад, до сих превалирует подход, основанный на так называемом балльном методе, реализованном в целом ряде международных стандартов и программных продуктов, таких как с программный продукт COBRA или программный продукт, реализующий метод CRAMM (метод CCTA[2] – Risk Analysis & Management Method , то есть метод анализа и контроля рисков), программный продукт RiskWatch, российский продукт АванГард и др. Наиболее широко известен и применяем метод CRAMM, в котором как размер ожидаемого ущерба, так и возможности реализации угроз оцениваются баллами. Однако недостатки этого подхода состоят в том, что, во-первых, некорректным оказывается суммирование разнородных ущербов, которые могут быть не только финансовыми или материальными, экономическими и даже экологическими, пересчитываемыми в финансовый ущерб, но ущербом здоровью людей и даже связанным с их гибелью, ущербом репутации предприятия, организации, органа власти или моральным ущербом, которые достаточно сложно оценить количественно. Во-вторых, оценка ущерба в данном случае является прогнозной, что существенно осложняет разработку соответствующих моделей и методик. В-третьих, в этих продуктах не учитывается фактор времени при оценке возможностей реализации угроз, что может приводить к некорректным выводам. В-четвертых, данный подход при оценке возможностей реализации угроз не привязан к применяемым мерам защиты и реализуемым в них функциям безопасности, что фактически не позволяет оценивать их эффективность.

Применительно к оценке возможных ущербов это обусловило разработку иного подхода, суть которого состояла в модификации балльного метода на основе парадигмы предельно допустимого ущерба и построения соответствующих шкал оценки с использованием элементов теории нечетких множеств. При этом, если ущерб оценивается по вербальной шкале, то на ней определяется точка предельного ущерба и все ущербы выше этой точки рассматриваются как недопустимые. Далее предельной точке ставится в соответствие верхняя граница числовой шкалы и затем по числовой шкале определяется относительный возможный ущерб (другое название – индекс ущерба). Если полагать, что недопустимый ущерб для любого вида ущерба в относительных величинах равен 1, то можно суммировать разнородные ущербы, рассчитанные по универсальной шкале. Пример взаимосвязи таких шкал приведен на рисунке 2.

Следует подчеркнуть, что оценка ущерба является условной в том смысле, что предельный ущерб отражает представление конкретного обладателя информации о ее важности для самого обладателя. Вместе с тем данный подход позволяет суммировать разнородные ущербы.

Применительно к оценке возможностей реализации угроз безопасности информации перспективы развития методического обеспечения связаны с построением формальных моделей процессов реализации угроз на сетевом, системном, прикладном и микропрограммном системно-технических уровнях. Надо сказать, что математический аппарат для

[2] CCTA (Central Computer and Telecommunications Agency) Центральное агентство по компьютерам и телекоммуникациям Великобритании

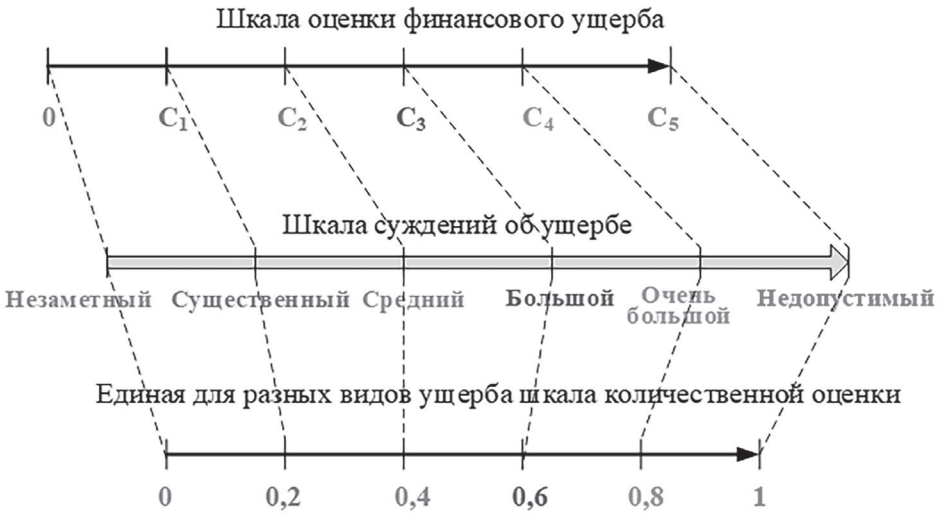


Рисунок 2. Взаимосвязь шкал оценки различных видов ущерба с универсальной шкалой

такого моделирования сегодня имеется. На его основе сегодня уже разработаны весьма разнообразные модели: как детерминированные, так и учитывающие всевозможные факторы неопределенности. Но особое внимание уделяется разработке стохастических моделей динамики реализации угроз во времени, позволяющих оценить возможности реализации угроз во времени, возможности опережения мерами защиты процессов реализации угроз и эффективность защиты путем сравнения возможностей реализации угроз без мер и при применении мер защиты. В основе этих моделей лежат аппарат марковских и полумарковских процессов, теория сетей Петри-Маркова, теория графов, математическая логика и теория предикатов и др.

Вместе с тем, при разработке таких моделей мы столкнулись с достаточно сложной ситуаций, суть которой состоит к следующем.

Сегодня каждую неделю выявляется и заносится в Банк данных угроз ФСТЭК России более 100 уязвимостей системного и прикладного ПО. Соответственно необходимо проводить анализ возможности их эксплуатации, то есть обосновывать возможности реализации соответствующих угроз. Даже применительно к одной какой-либо ИС провести такой анализ сложно, а если это делать для многих ИС и исследовать возможные траектории проведения компьютерных атак, то объем работ возрастает в сотни раз и без автоматизации в этом случае просто не обойтись. Например, даже для небольшого фрагмента АСУ ТП количество элементарных действий (техник), которые должны быть выполнены при компьютерных атаках на SCADA-сервер, достигает 64, а для больших информационных систем составляет нескольких тысяч, при этом время анализа может достигать сотни дней и более (рисунок 3).

В связи с этим крайне важным становится направление создания специальных экспертных систем, то есть программных комплексов, которые позволили бы путем введения необходимых исходных данных об ИС (назначении, архитектуре, составе системного и прикладного ПО и др.) формировать перечень актуальных угроз безопасности информации с учетом рисков их реализации в конкретных ИС, в том числе и прежде всего рисков реализации компьютерных атак, которые могут осуществляться внешними и внутренними нарушителями. Базы данных таких экспертных систем могли бы пополняться из банка данных угроз ФСТЭК России. В такие экспертные системы должны быть заложены и математиче-

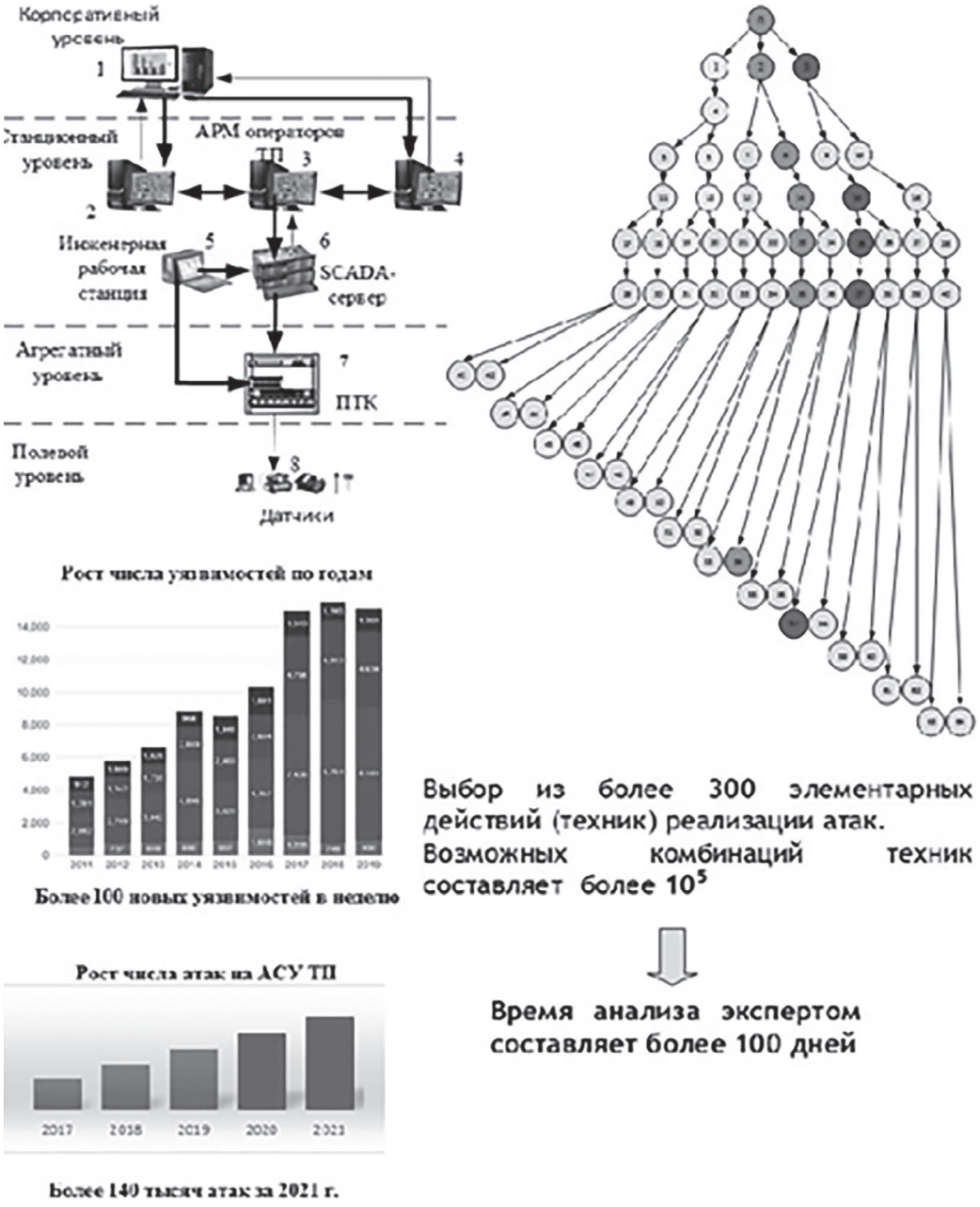


Рисунок 3. Рост размерности задачи анализа уязвимостей и угроз

ские модели оценки возможного ущерба при реализации каждой угрозы, и математические модели процессов реализации каждой угрозы во времени, в том числе с учетом применения предлагаемых мер и средств защиты, и модели количественной оценки эффективности защиты как от отдельных, так и от совокупности выбранных угроз. Задача весьма непростая, но вполне решаемая.

Соответствующие экспертные системы нужны и для обоснования требований по защите информации в ИС, в том числе требований к мерам, средствам и системам ЗИ в интересах парирования всех выявленных в ИС актуальных угроз. Сегодня формирование требований основывается на простом алгоритме, реализуемом экспертным путем, суть которого

состоит в последовательном выполнении процедур определения требуемого состава мер защиты, показанных на рисунке 4.

Рисунок 4. Порядок определения мер защиты информации в ИС
(на примере ГИС в соответствии с Приказом ФСТЭК России от 11.02.2013 г. №17)

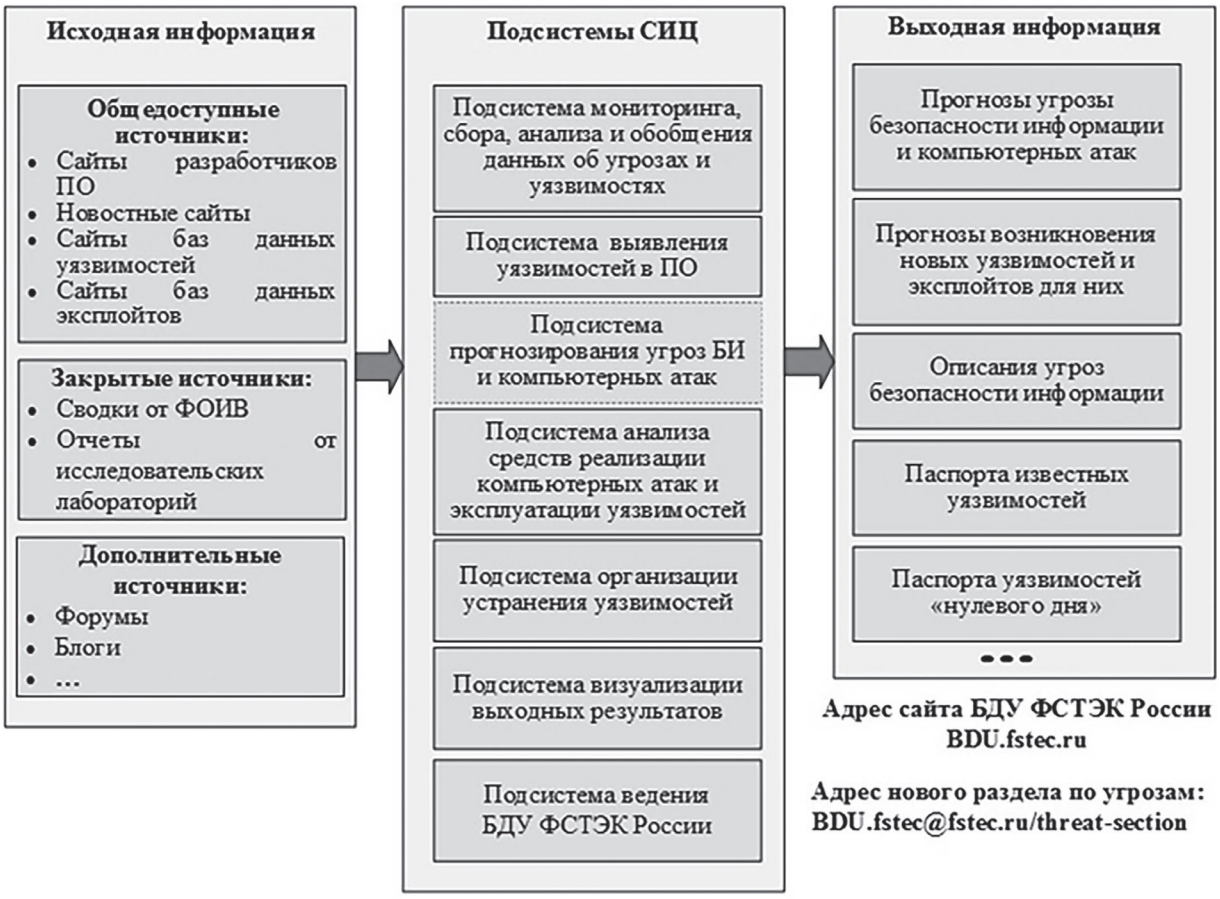


Рисунок 5. Ситуационный исследовательский центр

Однако при этом количественное обоснование таких требований сегодня фактически отсутствует, а эффективность выбираемых мер защиты не оценивается. Применительно к техническим мерам считается, что, если реализующие их средства защиты сертифицированы, то достигаемая эффективность достаточна. Но даже при этих очень серьезных ограничениях возникают проблемы, связанные с охватом всего множества уязвимостей системного и прикладного программного обеспечения, актуальных угроз безопасности информации в ИС и способов их реализации, адаптации, уточнения и дополнения базового набора мер защиты и тем более построения систем защиты информации в ИС.

Вместе с тем разработка полнофункциональных экспертных систем для анализа угроз и обоснования требований представляет собой весьма сложную задачу, решение которой целесообразно проводить поэтапно. Эта работа уже началась с создания достаточно простых программных комплексов для целого ряда подсистем развернутого в нашем институте ситуационного центра для ведения Банка данных угроз безопасности информации ФСТЭК России, адрес сайта которого приведен на рисунке 5.

В частности, в свете изложенного весьма интересным является новый раздел по угрозам, адрес которого приведен ниже. В нем содержится специальное программное средство, позволяющее по вводимым, в том числе в удаленном режиме, то есть по сети Internet, исходным данным об ИС и составным программно-аппаратным элементам (модулям) формировать в автоматическом режиме перечень актуальных угроз и их описание.

Следующими шагами в этом направлении станет создание программных средств, позволяющих на основе сформулированных требований формировать состав, структуры и алгоритмы функционирования систем защиты информации, а затем необходимо перейти к внедрению количественных методов оценке эффективности средств и систем защиты и к обоснования количественных требований к ним, а также к развитию методического обеспечения организации и ведения контроля, сертификационных испытаний средств защиты и аттестации систем защиты информации.

ВОПРОСЫ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.056.53

ОБЛИК СИСТЕМЫ СБОРА И ОБРАБОТКИ ДАННЫХ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВЫЯВЛЕНИИ КИБЕРАТАК В ИНФОРМАЦИОННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

М.А. БАБИЧ

Министерство обороны Республики Беларусь
г. Минск, *220034,* Республика Беларусь

В соответствии с подпрограммой «Инфраструктура цифрового развития» Государственной программы «Цифровое развитие Беларуси на 2021-2025 годы» в интересах Вооруженных Сил спланировано оборудование объектов Министерства связи и информатизации Республики Беларусь пунктами выделения каналов связи и разработка требований, строительство и ввод в эксплуатацию нескольких ведомственных центров обработки данных (ЦОД) [1].

Создание в интересах Вооруженных Сил нескольких ведомственных ЦОД наряду с передачей в эксплуатацию выделенных каналов электросвязи внесут изменения в существующую систему защиты информации ведомственных информационных сетей и систем.

В настоящее время в сетевой инфраструктуре ежесуточно фиксируются множество событий, которые могут свидетельствовать о вероятных инцидентах информационной безопасности, таких как нарушение регламентов и политик пользователями, несанкционированном доступе в информационные сети, недекларированной сетевой активности специального программного обеспечения.

Для централизованного сбора и анализа событий в крупных корпоративных сегментах принято использовать решения класса security information and event management (SIEM). Основная задача SIEM-системы – не просто собрать информацию о событиях с различных источников – сетевых устройств, приложений, журналов операционных систем, средств защиты, но и автоматизировать процесс обнаружения инцидентов, а также своевременно информировать о них специалистов по безопасности [2].

SIEM-системы традиционно применяются для решения проблемы накопления и оперативной обработки данных о событиях безопасности. Однако область применения SIEM-решений этим не ограничивается. Кроме того, с помощью SIEM-систем решаются такие важные задачи, как:

- выявление и расследование инцидентов информационной безопасности;
- инвентаризация активов и ресурсов информационной системы;
- контроль защищенности информационных ресурсов;
- мониторинг работы системы в условиях реальной ИТ-инфраструктуры;
- контроль и создание отчетов (диаграмм) о состоянии защищенности информационных ресурсов.

Обработка данных событий информационной безопасности начинается с подключения источников, которые генерируют разнородные события. Для получения наиболее полного представления о том, что происходит в сетевой инфраструктуре, планируется подключить все имеющиеся источники.

Для информационных сетей Вооруженных Сил, в большинстве случаев, такими источниками являются:

- средства антивирусной защиты;
- средства криптографической защиты;
- серверные операционные системы;
- активное коммутационное оборудование;
- системы идентификации и аутентификации пользователей;
- системы хранения и передачи файлов;
- системы виртуализации;
- системы обнаружения и предотвращения вторжений;
- системы обнаружения и предотвращения утечек информации;
- отдельные автоматизированные рабочие места пользователей.

Для сбора наиболее полных данных со всех источников планируемая к внедрению SIEM-система должна уметь взаимодействовать с широким спектром сетевых протоколов и технологий сетевого взаимодействия: syslog, WMI, RPC, SSH, ODBC и другими. В SIEM-систему будет поступать информация о событиях, определенных ведомственными политиками аудита (например – вход в систему, доступ к объектам системы, изменение привилегий пользователей, создание, изменение или удаление файлов заданного типа, подключение устройств, запуск сетевых служб, изменение конфигурации узла).

В зависимости от категории и типа события подразделения кибербезопасности Вооруженных Сил выбирают сценарий (метод) реагирования. В таблице 1 представлена общая классификация событий информационной безопасности при выявлении вероятных кибератак на информационные системы Вооруженных Сил.

Источники события	Категория события	Тип события
Прокси-серверы с контролем контента Средства защиты веб-трафика Средства защиты почты Средства защиты конечных узлов со встроенными модулями контроля веб-ресурсов и электронной почты Антивирусные средства защиты Средства обнаружения и предотвращения вторжений	Заражение вредоносным программным обеспечением (malware)	Внедрение в контролируемый информационный ресурс модулей ВПО (malware infection)
	Распространение вредоносного программного обеспечения (malware distribution)	Использование контролируемого информационного ресурса для распространения ВПО (malware command and control)
		Попытки внедрения модулей ВПО в контролируемый информационный ресурс (infection attempt)

Межсетевые экраны Системы обнаружения и предотвращения вторжений Системы выявления и блокировки сетевых DoS-атак	Нарушение или замедление работы контролируемого информационного ресурса (availability)	Компьютерная атака типа “отказ в обслуживании”, направленная на контролируемый информационный ресурс (dos)
		Распределенная компьютерная атака типа “отказ в обслуживании”, направленная на контролируемый информационный ресурс (ddos)
		Несанкционированный вывод информационный ресурс из строя (sabotage)
		Непреднамеренное (без злого умысла) отключение информационный ресурс (outage)
Средства защиты конечных узлов Сканеры уязвимостей Средства обнаружения и предотвращения вторжений	Несанкционированный доступ в систему (intrusion)	Успешная эксплуатация уязвимости в контролируемом информационном ресурсе (application compromise)
		Компрометация учетной записи в контролируемом информационном ресурсе (account compromise)
Межсетевые экраны Средства обнаружения и предотвращения вторжений Средства защиты конечных узлов	Попытки несанкционированного доступа в систему или к информации (intrusion attempt)	Попытки эксплуатации уязвимости в контролируемом информационном ресурсе (exploit attempt)
		Попытки авторизации в контролируемом информационном ресурсе (login attempt)

Средства обнаружения и предотвращения вторжений Сканеры уязвимостей и средства аудита Антивирусные средства защиты	Сбор сведений о контролируемой системе (information gathering)	Сканирование информационного ресурса (scanning)
		Прослушивание (захват) сетевого трафика контролируемого информационного ресурса (traffic hijacking)
		Социальная инженерия, направленная на компрометацию информационного ресурса (social engineering)
Системы предотвращения утечек данных из информационной системы	Нарушение безопасности информации (information content security)	Несанкционированное разглашение информации, обрабатываемой в контролируемом информационном ресурсе (unauthorised access)
		Несанкционированное изменение информации, обрабатываемой в контролируемом информационном ресурсе (unauthorised modification)
Сканеры уязвимостей и средства аудита	Уязвимость (vulnerability)	Наличие уязвимости или недостатков конфигурации в информационном ресурсе (vulnerability)

Таблица 1. Общая классификация событий информационной безопасности

Для обнаружения кибератак на ранней стадии необходимо знать обо всем, что происходит в сетевой инфраструктуре. Для этого нужно собирать как можно больше информации о событиях, ведь чем полнее ведется сбор событий и чем больше источников подключено, тем больше шансов своевременно выявить подозрительную активность, принять меры по пресечению кибератаки и минимизировать негативные последствия.

В свою очередь, большой объем регистрируемых данных в обязательном порядке требует автоматизированной обработки. SIEM-система использует корреляцию, чтобы обработать и связывать вместе собранные данные, выявлять шаблоны, указывающие на инцидент, а также служит основой для расследования инцидентов. Если дополнительно задействовать систему глубокого анализа трафика (решение класса NTA/NDR), то это позволит отслеживать подозрительную активность не только на узлах, но и в сетевом трафике.

Список литературы

1. О государственной программе «Цифровое развитие Беларуси на 2021 – 2025 годы» [Электронный ресурс]: Пост. Сов. безоп. Респ. Беларусь от 2 февр. 2021 г. № 66 // Нац. Правовой Интернет-портал Респ. Беларусь. – Режим доступа: https://pravo.by/document/?guid=12551&p0=c22100066&p1=1. – Дата доступа: 2.09.2021.
2. СТБ 34.101.74-2017 Информационные технологии. Системы сбора и обработки данных событий информационной безопасности. Общие требования. [Электронный ресурс] // Интернет-магазин БелГИСС. – Режим доступа: https://shop.belgiss.by/ru/gosudarstvennye-standarty/stb-34-101-74-2017 . – Дата доступа: 2.09.2021.

УДК 621.391.825

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 микроэлектронную элементную базу. Воздействие ПЭМП представляет особую опасность для автоматизированных цифровых систем управления ответственными технологическими процессами (АСУ ТП) на транспорте, энергетике , химических производствах.

Это обусловлено непредсказуемым поведением объектов управления при воздействии ПЭМП, приводящим к катастрофам и авариям и связанными с ними потерей жизни людей, огромным материальным ущербом и загрязнением окружающей среды.

Под преднамеренной электромагнитной помехой, 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.

Техническими средствами создания ПЭМП, как правило, являются специальные генераторы сверхкоротких электромагнитных импульсов, как большие стационарные, так и малогабаритные переносные.

Наибольшую опасность для цифровых ИТ систем и АСУ ТП представляют малогабаритные переносные наносекундные импульсные генераторы, излучающие энергию в диапазоне до 10 ГГц. Воздействие таким генератором с близкого расстояния может вывести из строя до 20 компьютеров.

Это связано как с высоким быстродействием современных микроэлектронных компонентов, так и с низким значением напряжения пробоя переходов. Так, например, у запоминающих устройств пороговое напряжение составляет порядка 7 В, а логических интегральных микросхем на МОП-структурах от 7 до 15 В. При этом анализ отказов и повреждений в оборудовании цифровых систем не позволяет порой однозначно идентифицировать причину возникновения повреждений, так как причиной может быть как ПЭМП, так и непреднамеренные помехи, вызванные индуктированными перенапряжениями в цепях питания и другими природными и паразитными техногенными процессами.

Воздействие ПЭМП на цифровые информационные системы и АСУ ТП как правило приводят к нарушению требований по обеспечению как информационной, так и функциональной безопасности. При этом основную угрозу безопасности систем создает не столько несанкционированное раскрытие обрабатываемой информации, сколько нарушение штатного функционирования с последующим нарушением управления системами жизнеобеспечения и условий обеспечения безопасности ответственных технологических процессов.

Особое место среди автоматизированных систем управления технологическими процессами занимают современные микроэлектронные системы железнодорожной автоматики и телемеханики (СЖАТ) призванные обеспечивать в первую очередь безопасность движения поездов. Это обусловлено предъявляемым 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.

Кроме того, особое место СЖАТ обуславливается тем, что они обладают существенными особенностями, усложняющими защиту указанных систем от преднамеренных электромагнитных помех. Во-первых, системы железнодорожной автоматики и телемеханики являются распределенными, многоуровневыми. Количество точек возможного преднамеренного воздействия значительно возрастает. Во-вторых, воздействие на оборудование микроэлектронных и микропроцессорных СЖАТ может осуществляться по свободному пространству, что организуется проще, нежели воздействие по кабельным линиям. В-третьих, затруднительно создать периметры защиты мест размещения оборудования СЖАТ, особенно на перегонах и малых станциях.

Поэтому разработка методов обеспечения защиты микропроцессорной аппаратуры СЖАТ к ПЭМП, 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» (Безопасность железных дорог от электромагнитных атак), задачей которого является разработка превентивных мер по защите микроэлектронных и компьютерных СЖАТ от электромагнитных помех, в том числе и преднамеренного воздействия. В рамках проекта производится и разработка аппаратно-программных комплексов защиты СЖАТ. В проекте задействовано десять организаций из наиболее влиятельных стран Евросоюза. Координатором является Французский

институт науки и технологии транспорта (IFSTTAR). Однако в открытом доступе имеются лишь общие сведения по данному проекту.

Существуют два подхода к решению проблемы защиты микроэлектронной аппаратуры от преднамеренных электромагнитных помех. Первый подход – физическое моделирование воздействия ПЭМП на такую аппаратуру 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 ПЭМП 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 и микроэлектронного и микропроцессорного оборудования критических объектов информационной инфраструктуры к различным электромагнитным помехам. Эта же задача возникает в рамках проблемы анализа и прогнозирования стойкости микропроцессорной аппаратуры СЖАТ к ПЭМП.

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

Допустимо считать, что паразитная антенна – неоднородность выделяет из фронта волны ПЭМП импульс неизменной, по сравнению с импульсом на выходе генератора, формы с амплитудой, определяющейся условиями распространения. Иными словами, временные параметры импульса не изменяются [1]. Вся поглощаемая антенной мощность излучается внутрь корпуса аппаратуры СЖАТ. Такое предположение допустимо по принципу наихудших условий. Тогда амплитуда импульса, излучаемого внутрь корпуса, может быть найдена по балансу мощности антенны, выраженной через вектор Пойнтинга [2]

$$\Pi_{\text{прин}} A_{\text{эфф}} = \Pi_{\text{изл}} A_{\text{геом}}, \quad (1)$$

где $\Pi_{\text{прин}}$ – принимаемый вектор Пойнтинга, Вт/м^2; $A_{\text{эфф}}$ – эффективнаия площадь антенны, м^2, В; $\Pi_{\text{изл}}$ – излучаемый вектор Пойнтинга, Вт/м^2, $A_{\text{геом}}$ – геометрическая площадь антенны, м^2.

Амплитуда принимаемого импульса электромагнитного поля выражается формулой [2]

$$E_{m,\text{пр}} = \frac{FOM}{r} e^{-\gamma r}, \; FOM = \sqrt{60PG}, \quad (2)$$

где FOM – параметр антенны, численно равный амплитуде напряженности электрического поля антенны на расстоянии 1 метр в направлении максимального излучения [2], В/м; P – мощность генератора, Вт; G – коэффициент усиления анетнны генератора, r – расстояние, м; γ – коэффициент ослабления в воздухе.

В данном случае можно принять простейшую функцию ослабления электромагнитного излучения $F(r,\omega) = 1 \cdot e^{-\gamma r}$, так как воздействие ПЭМП предполагается с незначительного расстояния [3].

Вектор Пойнтинга принимаемого импульса имеет вид

$$\Pi_{\text{пр}} = \frac{FOM^2}{240\pi r^2} e^{-2\gamma r}. \quad (3)$$

Вектор Пойнтинга излучаемого импульса

$$\Pi_{\text{изл}} = \frac{E_{m\text{изл}}^2}{240\pi}, \tag{4}$$

где $E_{m\text{изл}}$ – амплитуда излучаемого внутрь корпуса импульса, В/м.

После подстановки (2), (3) и (4) в (1) получается формула для амлитуды излучаемого импульса

$$E_{m\text{изл}} = \frac{FOM}{r}\sqrt{K_{\text{и}}}e^{-\gamma r}, \tag{5}$$

где $K_{\text{и}}$ – коэффициент использования антенны.

Амплитуда напряжения, созданного на антенне импульсом ПЭМП $U_{m\text{изл}} = xE_{m\text{изл}}$, тогда

$$U_{m\text{изл}} = FOM\frac{x}{r}\sqrt{K_{\text{и}}}e^{-\gamma r}, \tag{6}$$

где x – характерный размер отверстия, м.

Импульс ЭСР наиболее просто аппроксимируется импульсом биэкспоненциальной формы [4]. Поэтому для напряжения ПЭМП заданной формы и амплитуды, рассчитанной по (6), необходимо определить амплитуду и временные параметры эквивалентного биэкспоненциального импульса ЭСР по условиям эквивалентности импульсов. Физическим процессам передачи энергии через паразитную антенну наиболее соответствует спектрально-энергетический способ вывода условий эквивалентности импульсов [5]

$$\begin{cases} W_1 = W_2 \\ \Delta f_1 = \Delta f_2 \end{cases}, \tag{7}$$

где W_1 и W_2 – энергии импульсов, Дж; Δf_1и Δf_2 – активные полосы частот, Гц.

Параметры импульса генератора имитатора ЭСР подбираются из следующих соображений. Длительность и временные параметры импульса генератора устанавливаются близкими к параметрам импульса, эквивалентного ПЭМП. Амплитуда импульса генератора-имитатора ЭСР и импульса, эквивалентного ПЭМП, связаны коэффициентом подобия

$$K_{\text{под}} = \frac{W_{\text{экв}}}{W_{ЭСР}} = \frac{U_{m\text{экв}}^2}{U_{mЭСР}^2}. \tag{8}$$

Если осуществить испытания аппаратуры СЖАТ импульсом генератора-имитатора ЭСР с подобранными таким способом параметрами, то по результатам испытания можно косвенно судить об устойчивости этой аппаратуры к соответствующему ПЭМП. Это обосновывается тем, что испытания осуществляются пропорционально-подобными импульсами. Появляется возможность исследовать наиболее интересующие проектировщика режимы воздействия ПЭМП, спрогнозировать пороговые области расположения источников ПЭМП и свойства источников. Кроме того, можно установить устойчивость аппаратуры СЖАТ к ЭСР. 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.

Вторым подходом является математическое моделирование процесса проникновения ПЭМП в корпуса аппаратуры микроэлектронных СЖАТ численными методами либо по аналитическим выражениям для электромагнитного излучения паразитных антенн-неоднородностей корпусов технических средств СЖАТ. Преимуществами этого подхода являются низкие затраты средств, сравнительно небольшие затраты времени, 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 современное ПО можно разработать 3D модель объекта испытаний (ОИ), учитывающую используемые в конструкции объекта материалы и параметры среды распространения.

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 ПЭМП, 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.

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

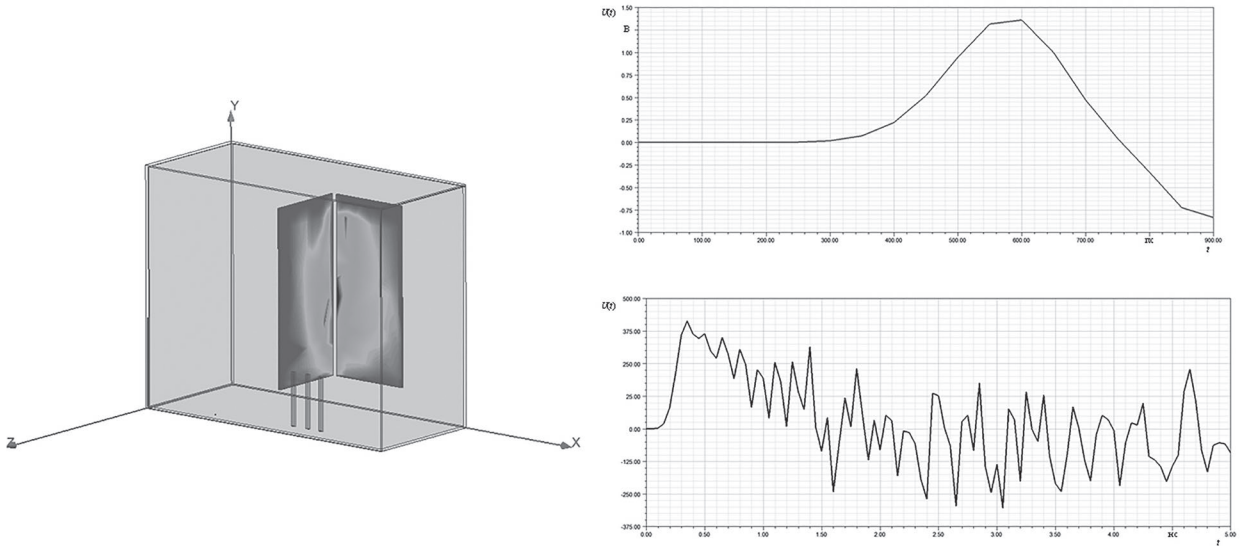


Рисунок 1. Представление результатов моделирования

При оценке защищенности ОИ численное моделирование может дать гораздо больше информации чем аналитический расчет, но разработка компьютерной модели ОИ достаточно трудоемкий процесс. Использование аналитического расчета целесообразно при нормировании параметров испытаний. Прогнозирования воздействия ПЭМП полезно при планировании процедуры натурных испытаний, так как позволяет осуществить целенаправленную подготовку экспериментов, исключить влияние человеческого фактора, охватить испытанием наиболее опасные режимы воздействия ПЭМП в пороговых областях. Проводить численное моделирование полезно, если аппаратура СЖАТ не прошла натурные испытания. В этом случае результаты моделирования применяются для поиска уязвимых мест. Для повышения помехоустойчивости потребуется проведение широкого комплекса расчетов большого числа вариантов конструкции аппаратуры СЖАТ, выполнить которые аналитически затруднительно.

Таким образом, проблема защиты СЖАТ от нового вида угроз – электромагнитного терроризма – может быть успешно решена путем комплексирования испытаний на устойчивость к электромагнитным помехам и совместного использования численного моделирова-

ния и аналитического расчета распространения ПЭМП. Это позволяет обеспечить требуемый уровень функциональной и информационной безопасности СЖАТ, как критически важных объектов информационной инфраструктуры.

Список литературы

1. Никольский, В. В. Теория электромагнитного поля / В. В. Никольский. – М.: Высшая школа, 1964. – 584 с.
2. Аполлонский, С. М. Расчеты электромагнитных полей / С. М. Аполлонский, А. Н. Горский. М.: Маршрут, 2006. – 992 с.
3. Кравченко, В. И. Радиоэлектронные средства и мощные электромагнитные помехи / В. И. Кравченко, Е. А. Болотов, Н. И. Летунова. М.: Радио и связь, 1987. – 255 с.
4. Кечиев, Л. Н. Защита электронных средств от воздействия статического электричества / Л. Н. Кечиев, Е. А. Пожидаев. М.: Издательский дом «Технологии», 2005. – 352 с.
5. Бочков, К. А. Элементы моделирования электромагнитной совместимости устройств железнодорожной автоматики и телемеханики / К. А. Бочков, Д. В. Комнатный. Гомель : БелГУТ, 2013. – 185 с.

УДК 004.056.5

О ЗАЩИТЕ ИНФОРМАЦИИ ПРИ ЕЕ УТЕЧКЕ ИЗ ВОЛС

С.В.КРУГЛИКОВ, В.А.ДМИТРИЕВ, Е.П.МАКСИМОВИЧ
Государственное научное учреждение «Объединенный институт проблем информатики Национальной академии наук Беларуси»,
220012, г. Минск, Республика Беларусь

Степень защищенности критически важных объектов от деструктивных информационных воздействий во многом определяется уровнем защищенности информационно-вычислительных и телекоммуникационных средств.

Одним из важнейших требований, предъявляемых к современным телекоммуникационным системам, является обеспечение скрытности и конфиденциальности связи. В волоконно-оптических линиях связи должна быть сформирована надежная, защищенная инфраструктура с использованием всех доступных средств и способов информационной защиты.

Одним из методов защиты информации от несанкционированного доступа при ее распространении в ВОЛС (волоконно-оптические линии связи) являются метод, основанный на использовании лазера, генерирующего импульсы оптического излучения столь малой длительности, что в пределах каждого импульса содержится один фотон, находящийся в состоянии линейной или круговой поляризации.

В современных системах ВОЛС самый перспективный способ передачи информации основан на модуляции интенсивности света. При этом способе передачи каналы утечки информации напрямую связаны с интенсивностью светового потока. Самый простой и действенный способ защиты информации при ее утечке из ВОЛС – снижение мощности модулированного сигнала. Снижение мощности модулированного сигнала может обеспечить полную защищенность информации только от пассивного съема. При активном съеме

полная защищенность информации не обеспечивется, но снижение мощности модулированного сигнала имеет большое значение, так как в этом случае нарушителю для перехвата потребуется выводить бóльшую мощность модулированного сигнала, что приведет к увеличению потерь в ВОЛС и упростит задачу обнаружения попытки съема. Для обнаружения слабого модулированного оптического излучения используется метод счета фотонов [1], который является одним из наиболее чувствительных методов регистрации слабого оптического излучения.

Поскольку оптическое волокно изготовлено из кварцевого стекла, то в качестве носителя информации необходимо использовать излучение полупроводникового лазера или лазерного диода в инфракрасной области на длинах волн 850 мкм, 1300 мкм и 1550 мкм. На указанных длинах волн затухание оптического излучения в оптическом волокне является минимальным.

Для передачи информативного сигнала в ВОЛС на большие расстояния используется одномодовое излучение полупроводникового лазера или лазерного диода, которое является импульсным и количество импульсов в неперекрывающихся временных интервалах статистически независимы. Статистическое распределение фотонов одномодового оптического излучения подчиняется распределению Пуассона [2,3].

Слабый оптический сигнал на выходе фотоприемника представляет собой последовательность флуктуирующих по амплитуде «одноэлектронных» импульсов [4]. Следует отметить, что статистика фотоэлектронов (фотоотсчетов), в плоскости чувствительного слоя фотоприемника повторяет статистику оптического излучения, падающего на фотоприемник, т.е. также является пуассоновской [5].

Тип шума аналогового фотоприемника, который преобразует демодулированное оптическое излучение, являющееся источником информации, которую необходимо защитить, в электрический сигнал (фотоэлектроны), зависит от частоты демодулированного оптического излучения. Если частота демодулированного оптического излучения $f \leq 100$ кГц, преобладающими шумами фотоприемника являются дробовые шумы с пуассоновской статистикой, а для частот демодулированного оптического сигнала $f > 100$ кГц преобладающими шумами фотоприемника являются тепловые шумы с гауссовской статистикой [6,7].

Тип шума цифрового фотоприемника, который преобразует демодулированное оптическое излучение, являющееся источником информации, которую необходимо защитить, в электрический сигнал (фотоэлектроны), зависит от скорости передачи информации по ВОЛС. Когда скорость передачи информации по ВОЛС $C \leq 500$ Мбит⁄с то преобладающими шумами цифрового фотоприемника являются дробовые шумы с пуассоновской статистикой, а для скоростей передачи информации по ВОЛС $C > 500$ Мбит⁄с , преобладающими шумами цифрового фотоприемника являются тепловые шумы с гауссовской статистикой [8].

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.

Полное скрытие информативных сигналов достигается только в том случае, когда $P_0 \le 0{,}3$ [9].

Для анализа аналоговых информативных сигналов следует использовать аналоговые фотоприемники.

В том случае, когда статистики сигнальных и шумовых фотоэлектронов являются пуассоновскими, то вероятность обнаружения модулированного оптического излучения и порог обнаружения модулированного оптического излучения определяются следующим

$$P_0 = \Phi\left[\sqrt{\frac{N \cdot S \cdot \overline{s_c}}{1+S}} - \frac{1}{\sqrt{1+S}} \cdot \Phi^{-1}(1 - P_{лт})\right], \quad (1)$$

$$n_0 = E\left[N \cdot \overline{s_ш} + \sqrt{N \cdot \overline{s_ш}} \cdot \Phi^{-1}(1 - P_{лт})\right], \quad (2)$$

где N – число фотоотсчетов,

$\overline{s_c} = \overline{I_c} \cdot T$ – среднее число сигнальных фотоэлектронов за время наблюдения T,

$\overline{s_ш} = \overline{I_ш} \cdot T$– среднее число шумовых фотоэлектронов, за время наблюдения T,

P_o – вероятность обнаружения,

$P_{лт}$ – вероятность ложной тревоги,

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

$\overline{I_ш}$ – средний поток шумовых фотоэлектронов,

T – длительность выборки (интервал наблюдения),

$S = \frac{\overline{s_c}}{\overline{s_ш}}$ – отношение сигнал/шум,

n_0 – порог обнаружения модулированного оптического излучения,

$\Phi(t) = \frac{1}{\sqrt{2 \cdot \pi}} \cdot \int_{-\infty}^{t} \exp\left(-\frac{x^2}{2}\right) dx$ – интеграл вероятности,

Φ^{-1} (t) – функция, обратная интегралу вероятности, удовлетворяющая соотношению $\Phi^{-1}[\Phi(t)] = t$,

E(y) – целая часть y.

В том случае, когда статистика сигнальных фотоэлектронов является пуассоновской, а статистика шумовых электронов – гауссовской, то вероятность обнаружения модулированного оптического излучения и порог обнаружения модулированного оптического излучения определяются следующим образом:

$$P_0 = \Phi\left[\frac{S \cdot \sqrt{N \cdot \frac{\overline{s_c}}{S+\overline{s_c}}} + \Phi^{-1}(1 - P_{лт})}{\sqrt{\frac{S^2}{S+\overline{s_c}} + \frac{2 \cdot S \cdot \overline{s_c}}{S+\overline{s_c}} + 1}}\right], \quad (3)$$

$$n_0 = 2 \cdot N \cdot \overline{s_ш} + \sqrt{N \cdot \overline{s_ш} \cdot (\overline{s_ш} + 1)} \cdot \Phi^{-1}(1 - P_{лт}). \quad (4)$$

Для анализа цифровых информативных сигналов следует использовать цифровые фотоприемники, в которых используются устройства бинарного квантования [10].

В том случае, когда статистика сигнальных фотоэлектронов является пуассоновской, а статистика шумовых электронов – гауссовской, то вероятность обнаружения модулированного оптического излучения и порог обнаружения модулированного оптического излуче-

ния с использованием критерия «хотя бы один фотоотсчет из N фотоотсчетов» определяются следующим образом:

$$P_o = 1 - \left\{A + S \cdot \left[A \cdot B^{1/n_0} - n_0 \cdot B \cdot \left(1 - B^{1/n_0}\right)\right]\right\}^N \cdot \exp\left(-S \cdot N \cdot B^{1/n_0}\right), \quad (5)$$

$$A = (1 - P_{лт})^{1/N}, \quad (6)$$

$$B = 1 - (1 - P_{лт})^{1/N}, \quad (7)$$

$$n_0 = \frac{\ln B}{\ln\left(\frac{\overline{s_ш}}{\overline{s_ш}+1}\right)}. \quad (8)$$

В том же случае, когда статистика сигнальных фотоэлектронов является пуассоновской, а статистика шумовых электронов – гауссовской, то вероятность обнаружения модулированного оптического излучения и порог обнаружения модулированного оптического излучения с использованием критерия «N фотоотсчетов из N фотоотсчетов» определяются следующим образом:

$$P_0 = \left\{1 - \left\{D + S \cdot \left[(1 - C) \cdot C^{1/n_0} - n_0 \cdot C \cdot \left(1 - C^{1/n_0}\right)\right]\right\} \cdot \exp\left(-S \cdot C^{1/n_0}\right)\right\}^N, \quad (9)$$

$$C = P_{лт}^{1/N}, \quad (10)$$

$$n_0 = \frac{\ln P_{лт}}{N \cdot \ln\left(\frac{\overline{s_ш}}{\overline{s_ш}+1}\right)}. \quad (11)$$

Список литературы

1. Ветохин С.С. *Одноэлектронные* фотоприемники / С.С.Ветохин, И.Р. Гулаков, А.Н. Перцев, И.В. – М.: Энергоатомиздат, 1986. – 246 с.
2. Гудмен Дж. Статистическая оптика / Дж. Гудмен. – М.: Мир, 1988. – 528 с.
3. 3. Шереметьев А.Г. Статистическая теория лазерной связи / А.Г.Шереметьев. – М.: Изд-во «Связь», 1971. – 264 с.
4. 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.
5. Клаудер Дж. Основы квантовой оптики / Дж. Клаудер, Э. Сударшан. – М.: Мир, 1970. – 430 с.
6. Александров С.Е. Влияние низкочастотных шумов на пороговую чувствительность фотодиодных фотоприемных устройств среднего ИК-диапазона в широкой полосе частот / С.Е.Александров, Г.А. Гаврилов, Г.Ю. Сотникова // Письма в ЖТФ. – 2014. – Т. 40. – В. 16. – С. 58-64.
7. Торшина И.П. Выбор приемника излучения при проектировании оптикоэлектронного прибора: учебное пособие / И.П.Торшина, Ю.Г. Якушенков. – М.: Изд-во МИИГАиК, 2017. – 58 с.
8. Шубин В.В. Информационная безопасность волоконно-оптических систем / В.В.Шубин. – Саров: РФЯЦ-ВНИИЭФ, 2015. – 257 с.
9. Хорев А.А. Оценка эффективности защиты информации от утечки по техническим каналам / А.А. Хорев // Специальная техника. – 2006. – № 6. – 53-61.
10. Клюев Н.Ф. Обнаружение импульсных сигналов с помощью накопителей дискретного действия / Н.Ф.Клюев. – М.: Изд-во «Советское радио», 1963. – 113 с.

УДК 004.056

ОБ ОЦЕНКЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В СОВРЕМЕННЫХ УСЛОВИЯХ

КУРИЛО А.П., к.т.н., доцент
ООО «Финансовые и бизнес консультанты»
Советник Вице-президента
по безопасности информационных систем

В конце февраля 2022 года неожиданно и тем не менее предсказуемо возникла задача отражения массированных атак на огромное количество субъектов информационной инфраструктуры РФ. Можно обсуждать, все ли возможности были использованы противоположной стороной и используются по сей день в ходе кибератак или нет. Скорее, еще нет, наверняка что-то еще лежит «за пазухой», но российскими специалистами уже получен достаточный опыт борьбы с проявившимися угрозами, о чем свидетельствует в принципе очень неплохая статистика инцидентов, вызванных кибератаками, а также выход серии рекомендаций государственных регуляторов и НКЦКИ. Позже были «сломаны» несколько организаций «второго и третьего плана» ну и, пожалуй, все. Причины этих неудач тоже известны: безответственное отношение к задачам защиты информационных ресурсов со стороны руководства, инсайдерство и безграмотный выбор подрядчиков при отсутствии какого-либо контроля со стороны организации–заказчика и ее службы информационной безопасности.

Естественно, на фоне в принципе довольно успешного в целом отражения атак, стали очевидны и слабости в системе защиты, которые можно разделить на управленческие (отсутствие должной ответственности и исполнительских ресурсов), и собственно слабостей систем защиты.

Рисунок 1.

И тут во весь рост встает задача оценки эффективности защиты. А эта задача, скажем прямо, не тривиальная.

Обратимся к фундаментальным основам управления.

Парадигма защиты предполагает, что защищенность, как специфическое состояние системы, возникает как ее способность преодолевать негативное воздействие внешней среды в виде воздействия угроз информационной безопасности через соответствующие атаки на уязвимости системы защиты. Для достижения целей защиты необходимо выделение необходимых ресурсов, необходимы адекватные требования по защите, настраивающие систему безопасности, и эффективное управление (рис.1).

Отметим также, что понятия регулирование и управление хотя и являются синонимами, существенно отличаются, как это следует из их определений[3]:

В условиях условно «мирного» времени, то есть Надо сказать, что кибервойна, по-существу, никогда и не прекращалась, однако ее интенсивность до 22. 02.2022 года была на порядки ниже. В этих условиях более – менее эффективно работала схема регулирования, представленная на рис. 2. О ее недостатках достаточно много сказано ранее, однако отметим, что в России в качестве схемы управления была принята парадигма «регулирования».

Цели, состав задач регулирования, виды регулирования и виды контроля приведены на рис. 3.

Анализ видов контроля привел к выводам, изложенным в таблице 1.

Информационная безопасность, как специфическое состояние системы, являясь многомерной сущностью, характеризуется следующими показателями:

- статической безопасностью, характеристики которой формируются на основании соответствующих оценок результатов аудита информационной безопасности и оценки соответствия требованиям по безопасности;
- динамической безопасностью, характеризующей реальную (текущую) безопасность системы, состояние ключевых элементов ее защиты, возможность выявлять и идентифицировать атаки, а также обрабатывать возникающие инциденты. Показатели динамической безопасности формируются прежде всего за счет оценки качества работы систем мониторинга и оперативного управления;
- отсутствием или наличием уязвимостей в защищаемой системе, объективные сведения о чем могут быть получены только через техническую проверку:
- готовностью объекта защиты в целом к отражению атак и действиям в условиях чрезвычайных ситуаций (результаты киберучений).

---

[3] (от *лат.* regulo – устраиваю, привожу в порядок) - *англ.* regulation; *нем.* Regulierung. 1. Приведение в порядок, упорядочение (механизма, деятельности и т. д.); руководство движением, направлением, действиями, отношениями и т. п. 2. Совокупность предписаний, исходящих от органа власти или управления и имеющих целью внести известный порядок в ту или др. сферу жизни. 3. Форма целенаправленного управляющего воздействия, ориентированного на поддержание равновесия в управляемом объекте и на его развитие посредством введения в него регуляторов (норм, правил, целей, связей).
Энциклопедия социологии, 2009

У**правление** (синоним понятия **менеджмент**) — процесс прогнозирования, планирования, организации, мотивации, координации и контроля, направленный на формулировку и достижение цели организации
Майкл Мескон, Майкл Альберт, Франклин Хедоури. Основы Менеджмента (Management) = Management / пер. Л. И. Евенко. — М.: Дело, 1997. — 704 с. — (Зарубежный экономический учебник). — 12 000 экз. — ISBN 5-7749-0047-9 (0060444150).

Рисунок 2.

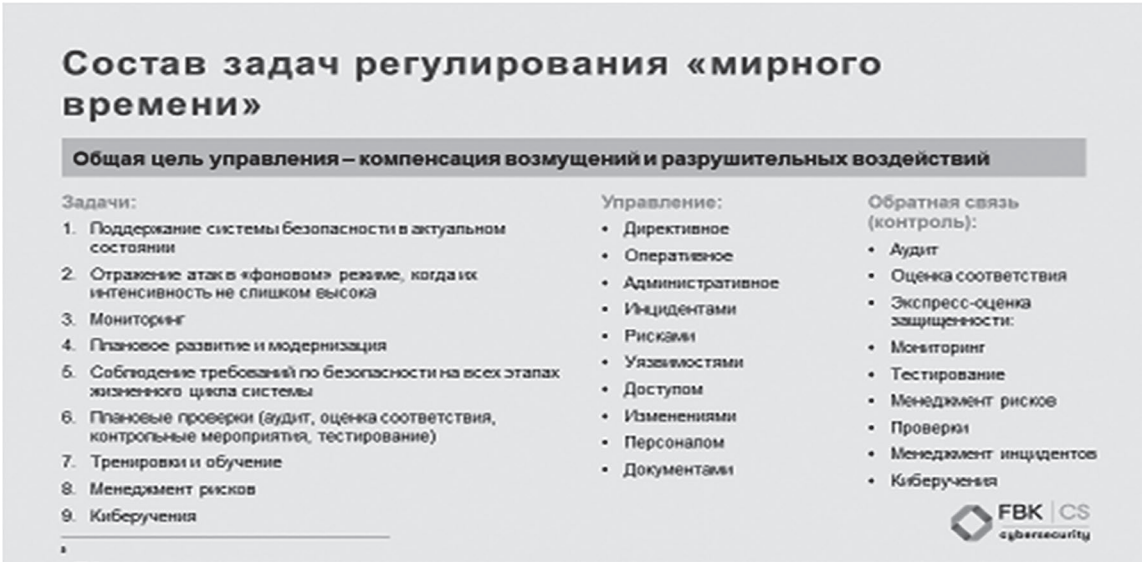


Рисунок 3.

Зададим несколько вопросов и ответим на них.

1. Информация о статической безопасности объекта важная и нужная информация? – Да, несомненно.
2. Это информация достаточная для получения уверенности в защищенности объекта? – Нет.
3. Дает ли эта информация полное знание о состоянии защищенности объекта? – Нет.
4. Дают ли проверки статического состояния системы (Аудит, оценка соответствия) уверенность в способности системы отразить атаку? – Нет.

Сравнительная характеристика эффективности и применимости видов контроля

№ № п/п	Вид контроля	Сфера регулирования	Регулярность	Нормативная база, требования	% реализации общей задачи защищенности	% эффективности защиты от атак	Что преимущественно оценивается
1	Аудит ИБ	Общая	Общая- не определено КФС - от 1 до 3 лет	Общая-COBIT КФС- СТОИББС	До 50	До 20	Статическое состояние
2	Оценка соответствия требованиям по безопасности	1. Общая 2. КФС	Общая- не определено КФС - от 1 до 3 лет	1. Общая, по документам ФСТЭК 2. КФС - по ГОСТ	До 70	До 40	Статическое состояние
3	Экспресс-оценка защищенности	Общая	Срочная, по указу ПРФ № 250	По оперативным данным?	5	До 50	Готовность к отражению атак
4	Инструментальное тестирование	Общая	Общая- не определено КФС - от 1 до 3 лет Срочная, по указу ПРФ № 250	Общая- не определено КФС - от 1 до 3 лет Срочная, по указу ПРФ № 250	15	До 80	Готовность к отражению атак
5	Мониторинг СОИБ	Общая	Требований нет	Не определено	До 10	До 80	Оперативное состояние системы
6	Контрольная проверка	Общая	На основании внутренних регламентов	нет	-	-	Подготовленность и работоспособность коллектива
7	Менеджмент рисков	КФС	Требований нет	Положение ЦБ, СТОИББС	3	10	Наличие рисков
8	Менеджмент инцидентов	КФС	Требований нет	СТОИББС	-	-	Готовность к обработке инцидентов
9	Киберучения	Общая	Требований нет	нет	-	До 80	Реальная готовность к отражению атак

Таблица 1.

Объем выполнения общей задачи защищенности и достигаемой эффективности защиты приведен в таблице. Для каждого вида контроля он не высок. И нельзя сказать, что задача повышения и обеспечения требуемого уровня защищенности решается методами контроля статического состояния защищенности объекта со 100% эффективностью. Практика показала, что существует довольно высокий риск реализации атаки на объект защиты. Поэтому практически все методики оценки защищенности базируются на вероятностных оценках защищенности, а критерии уровня защиты назначаются экспертным способом. Именно этот подход реализован в ГОСТ Р 57580.2-2018. Остальные методики проще, так как содержит только один критерий – 100% выполнения требований. Но оказывается этого тоже недостаточно. Возникает парадоксальная ситуация: 100% выполнения требований по безопасности, выполненные для системы, находящейся в статическом состоянии, не гарантируют еще достижения ее высокого уровня защищенности. Именно поэтому практика интуитивно наработала целых 9 видов различных контролей, предназначенных для получения знания о следующих видах состояния безопасности системы:

- Статическом состояния системы защиты;
- Оперативном (динамическом) состоянии системы защиты, прежде всего способности к выявлению и отражению атак;
- Наличии и числе уязвимостей, полученные инструментальным способом;
- Наличии рисков информационной безопасности (как процедуры оценки статического состояния), а также готовности к обработке возникающих инцидентов;
- Готовности персонала;
- И наконец, реальной готовности и способности отражать атаки.

Только по завершении всех этих контролей можно говорить о получении объективной картины в части защищенности информационной системы и способности ее системы защиты противостоять атакам.

Методически, общий подход к обеспечению безопасности объектов информационной инфраструктуры инфомационного объекта может выглядеть как последовательность обозначенных девяти видов контролей при обязательной реализации мер по улучшению системы на каждом этапе:

a. В плоскости «статической» безопасности:
   - Аудит информационной безопасности с подготовкой общей оценки «зрелости» системы информационной безопасности и рекомендаций на проведение ее стратегических улучшений;
   - Оценка соответствия объектов информационной инфраструктуры системы требованиям защищенности с выведением показателя защищенности и устранением выявленных недостатков;
   - Реализация процедуры менеджмента рисков.

b. В плоскости «динамической» безопасности:
   - Развертывание эффективной системы мониторинга текущего состояния объектов информационной инфраструктуры в виде SOC и его основной составляющей SIEM с реализацией процедур менеджмента инцидентов.

c. В плоскости «менеджмента уязвимостей»:
   - Инструментальная проверка уязвимостей системы (pen-тестирование)

d. В плоскости оценки готовности коллективов (персонала функциональных подразделений ИБ и IT) к готовности к отражению атак
   - киберучения.

Нужно сказать, что в условиях развернувшейся кибер-санкционной войны, решить задачу такого комплексного контроля весьма сложно, если возможно. Нет ни времени, ни ресурсов. В этих условиях нужно выбирать главное. А главным является способность и готовность к отражению атак на самые ценные ресурсы и функциональность.

Как показывает опыт, в условиях жесткого противостояния прежде всего модернизируется система управления, которая начинает представлять из себя конструкцию, основные контуры которой представлены на рис. 4. Эта система характеризуется прежде всего рез-

Рисунок 4.

ким усилением ответственности руководителей за обеспечение ИБ и сокращением числа контрольных мероприятий.

Состав задач управления в условиях кибервойны представлен на рис. 5. В этой ситуации существенным образом претерпевают изменения цели управления. Таких целей оказывается всего две:

1. Подготовка среды (объектов информационной инфраструктуры) и ее главной составляющей – объектов КИИ к отражению кибератак в условиях прогнозируемого роста интенсивности сложных целевых длительных атак (APT) через реализацию оперативных требований по безопасности, сформулированных уполномоченными организациями.
2. Оценка уровня защищенности среды в целом, то есть, получение сведений о том, как объекты подготовились к реальному отражению атак.

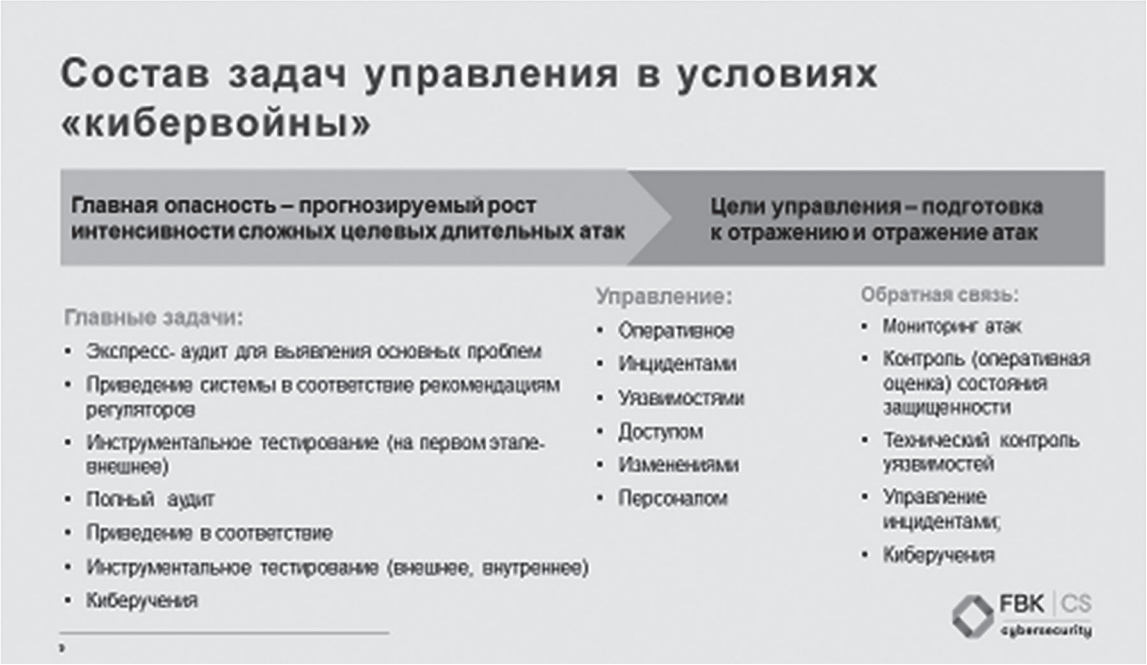


Рисунок 5.

Таким образом, в условиях реального давления со стороны недружественной среды, дефицита времени и ресурсов возникает экспресс-задача быстрого приведения системы в состояние готовности к реальному отражению атак и оценки уровня подготовки к этому.

Эту задачу можно решить только путем сокращения объема требований и контролей. Поэтому возникла и сейчас реализуется идея обработки ограниченного объема требований по безопасности только для самых важных, критических, или говоря другим языком, неприемлемых для объекта защиты событий. А таких событий не может быть много. Правда возникает вопрос, как относится к тому, что если мы не будем допускать неприемлемые события, допустимы ли все остальные? А они неминуемо наступят. Тут должна возникнуть некое ранжирование, на основании которого мы должны классифицировать и оценивать эти события. Так, например, руководитель, ответственный за состояние информационной безопасности организации будет нести ответственность за то, что у возникли незначительные инциденты, связанные с «проколом» системы защиты, но не недопустимых событий?

Это на войне хорошо: командир танка, в который попала ракета, но ничего в нем не сломала, герой. Но ведь с другой стороны, он ведь подставил машину под удар, не принял вовремя меры, значит в принципе, нужно было его наказать.

Ну а нам не следует забывать, что нужно еще провести техническое тестирование и очень желательно – киберучения, на что сейчас похоже внимания обращается еще недостаточно.

Далее. Задачи классической оценки защищенности через аудит информационной безопасности и оценки соответствия никто не отменял и не отменит. Нужно будет проводить и эту работу. И не забывать, что в это время уже в полный рост встанет тема импортозамещения и ее придется рассматривать в совокупности со всеми остальными задачами. Но это уже проблематика второго этапа, который может наступить несколько позже, через несколько месяцев, а может и через год. И снова нужно не забыть, что нужно будет еще снова провести техническое тестирование и очень желательно – киберучения.

В заключение необходимо сказать, что уже те изменения в методических подходах к управлению состоянием информационной безопасности в текущей ситуации, выявили вопросы, которые неминуемо необходимо решать в недалеком будущем. К ним следует отнести:

- Оптимизацию управления системой информационной безопасности с отходом от «регуляторного» метода управления;
- Интеграцию в общую систему оценки уровня защищенности результатов частных оценок по обозначенным выше направлениям;
- Ранжирование инцидентов и их последствий;
- Включение в систему оценок результатов киберучений;
- Выстраивание понятной и цепочки контролей и проверок с учетом мучительных, плохо методически обеспеченных проверок некоторых регуляторов.

УДК 004.31, 004.056.5, 004.522, 004.93′1, 519.2, 57.087, 612.087

ПОРТАТИВНЫЙ ЗАЩИЩЕННЫЙ КОММУНИКАЦИОННЫЙ МОДУЛЬ С БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИЕЙ НА ОСНОВЕ НЕЧЕТКОГО ХРАНИЛИЩА

Г.Ф. АСТАПЕНКО, П.В. КУЧИНСКИЙ, М.И. НОВИК, Н.А. РАЩЕНЯ
Научно-исследовательское учреждение «Институт прикладных физических проблем имени А.Н. Севченко» Белорусского государственного университета
Минск, Республика Беларусь

Представлена базовая архитектура и аппаратно-программное обеспечение портативного защищенного коммуникационного модуля (ПЗКМ). Модуль позволяет взаимодействовать с другими ПЗКМ в пределах локальных зон ближнего взаимодействия (посредством WiFi) и дальнего взаимодействия (посредством сотовых сетей 3G/4G). Базовая архитектура ПЗМК представляет собой модифицируемый и масштабируемый набор функциональных модулей, обеспечивающих безопасное формирование, обработку и передачу мультимедийных

данных. Программные компоненты ПЗКМ организованы в иерархическую структуру взаимодействия от верхнего прикладного уровня до уровня встроенной операционной системы. Для целей защиты и надежного использования ПЗКМ предложена схема биометрической аутентификации на основе отпечатка пальцев и парольной фразы, при этом используются механизмы нечеткого хранилища и возобновляемых биометрических шаблонов. Приведены достоинства предложенной схемы.

1 Архитектура портативного защищенного коммуникационного модуля (ПЗКМ)

ПЗКМ представляет собой компактное устройство, которое в одном из прикладных применений может служить надежным, безопасным ассистентом пользователя при формировании, передаче и приеме конфиденциальной информации [1].

На рисунке 1 представлен функциональный состав основных компонентов ПЗКМ.

Ядром модуля является процессор TI AM4378 на основе ARM архитектуры. Он содержит блоки обработки данных, их хранения, а также периферийный узел, осуществляющий интерфейс связи с внешними источниками и приемниками потоков данных и сигналов.

Несмотря на то, что внутри процессора находится встроенный криптомодуль, для повышения надежности и безопасности ПЗКМ содержит дополнительные аппаратные модули крипто-ускорителя и физического генератора случайных числовых последовательностей (ГСЧП). Модуль крипто-ускорителя реализует арифметические и алгебраические функции обработки больших чисел, а также операции над точками эллиптической кривой.

Для реализации беспроводного интерфейса на основе технологии WLAN используется комбинированный (WiFi/Bluetooth) чип TI – WL1835 MODCOM8B, а для реализации беспроводной связи ближнего поля (в пределах 10 см) (NFC) – чип TITRF7970A.

Для обеспечения связи в 3G/4G сети применяется встраиваемый Skywire сотовый модем [2], подключаемый к процессору посредством интерфейса USB2/UART.

Для обеспечения средствами мультимедийной обработки данных ПЗМК содержит встроенные модули: аудио кодек, видео камеру, К ПЗМК также может подсоединяться сенсорный экран.

Для реализации сервиса безопасности процедур локальной и удаленной аутентификации ПЗКМ дополнен встроенным компонентом сканирования и обработки отпечатков пальцев SLK20S фирмы ZKTeco [3], взаимодействие с которым на аппаратном уровне осуществляется через последовательный интерфейс UART (115200 бит/с). Основными критериями выбора данных модулей среди других подобных моделей от различных производителей, являются: высокие технические характеристики; обеспечение программным инструментарием (SDK) и соответствующей документацией; поддержка защиты от подделок отпечатков.

Для поддержки аудио интерфейса на аппаратном уровне в ПЗКМ реализуется двумя модулями: мультиканальный аудио последовательный порт (McASP – Multichannel Audio Serial Port) процессора; аудио кодек TLV320AIC3110. McASP функционирует как общего назначения последовательный аудио порт, оптимизированный для мультиканальных аудио приложений. Аудиокодек TLV320AIC3110 оснащен высокопроизводительным аудиокодеком с 24-битным стереофоническим воспроизведением и функцией монофонической записи. Устройство объединяет несколько аналоговых функций, таких как интерфейс микрофона, драйверы наушников и динамиков.

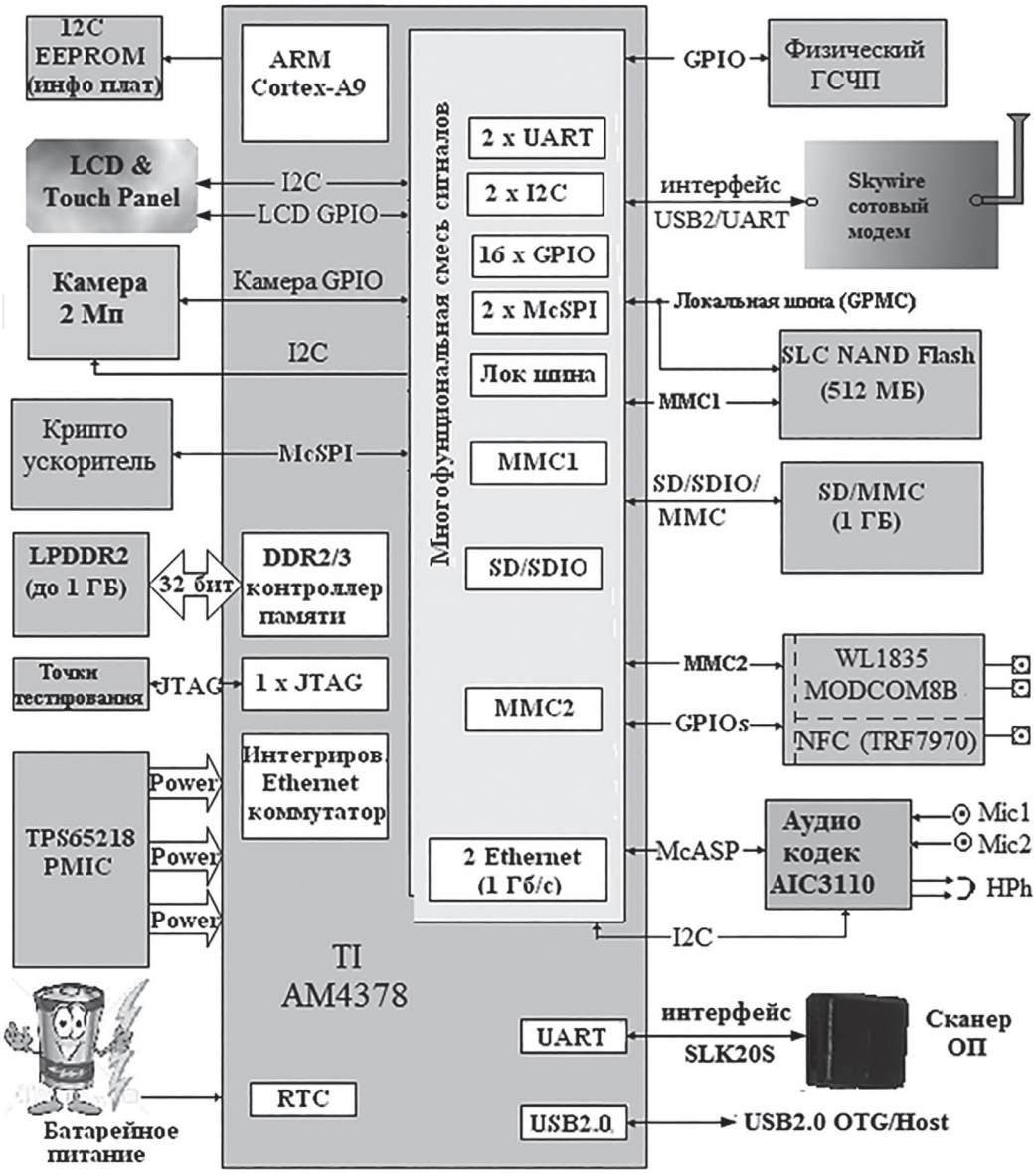


Рисунок 1. Функциональные компоненты ПЗКМ

2 Отменяемая биометрическая аутентификация на основе нечеткого хранилища

Отменяемая биометрия направлена на усиление защиты конфиденциальности и безопасности шаблонов в существующих биометрических системах [4]. При этом биометрический шаблон искажается таким образом, что исходные данные недоступны злоумышленнику, но все же может быть выполнено распознавание личности.

Безопасность системы аутентификации можно усилить, используя биометрическую систему, вместо традиционного метода аутентификации, такого как удостоверение личности (ID) и пароль, которые можно легко украсть. Среди всех модулей биометрической системы, которым необходимо обеспечить безопасность, защита биометрических шаблонов нуждается в наибольшем внимании из-за чувствительности биометрических данных, хранящихся в форме шаблона. Для обеспечения защиты шаблонов был разработан ряд методов.

Нечеткое хранилище (fuzzy vault) [5] – это один из методов защиты шаблонов, основанный на криптосистеме. Целью метода нечеткого хранилища является защита ненадежных

данных с помощью биометрического шаблона таким образом, чтобы только сертифицированный пользователь мог получить доступ к секрету, предоставив действительные биометрические данные.

Нечеткое хранилище может быть процедурой по обеспечению безопасности криптографических ключей для симметричных криптосистем. Нечеткое хранилище защищает шаблон, а также ключ k, блокируя шаблон с помощью ключа, и законный пользователь может получить доступ к ключу только в том случае, если его шаблон пересекается с заблокированным. Нечеткое хранилище состоит из двух этапов: кодирования и декодирования. Секретный ключ кодируется (шифруется) в виде полинома p, коэффициенты которого представляют собой ключ. Вектор биометрических признаков V проецируется на полином, чтобы сформировать набор подлинных точек. Некоторые точки, называемые точками чафф (chaff), для повышения безопасности генерируются случайным образом и не должны совпадать с подлинными. Коллекция подлинных точек и точек chaff образует хранилище. На этапе декодирования производится разблокирование секретного ключа k'. Пользователь представляет свой собственный набор признаков V' и может разблокировать секрет k, если набор признаков V' в значительной степени совпадает с набором признаков V. Безопасность этого метода зависит от сложности полиномиальной регенерации (например, на основе интерполяции Лагранжа).

На рисунке 2 приведена обобщенная схема регистрации и аутентификации пользователя на основе хранилища секретных данных.

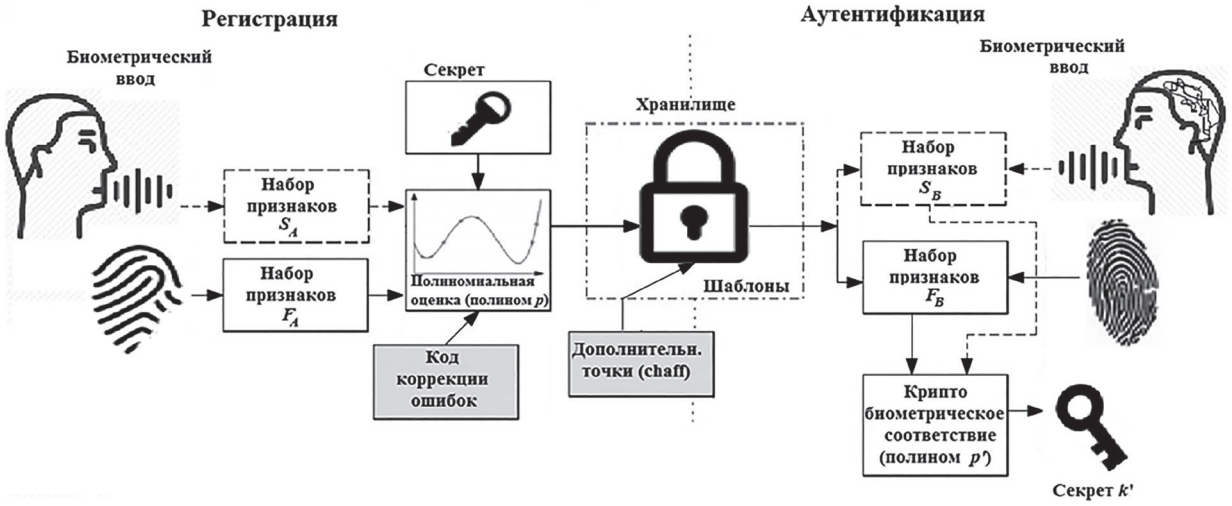


Рисунок 2. Нечеткая схема хранилища секретных данных

Функционирование предлагаемой схемы выполняется посредством следующих фаз и шагов.

Фаза регистрации в центре выпуска серии персональных устройств

1. Секретный ключ k (например, мастер-ключ) первоначально записывается в секретную память устройства.
2. В секретную память записывается дополнительная информация (например, идентификационный номер владельца персонального устройства, параметры широковещательного обмена в виртуальной частной сети (ВЧС) и др.).

Фаза инициализации

1. Вычисляется хэш-образ секретного ключа h(k).
2. Вводятся не менее трех раз изображения отпечатка пальца для формирования шаблона TF (Template Finger) (посредством преобразования набора признаков F_A).
3. Формируется нечеткий кодировщик GenF с помощью биометрического шаблона TF для скрытия k, при этом используется полиномиальное преобразование (p_1) и один из кодов исправления ошибок Cod_1 (БЧХ, Рида-Соломона или LDPC (Low Density Parity Check)). Следует отметить, что длина двоичной последовательности кодирования должна быть больше L бит, где L – приемлемый уровень безопасности).
4. Кодируется секретный ключ k с помощью GenF: k_{SF} = GenF(k, Cod_1, C_1), где C_1 – вспомогательная случайная последовательность дополнительных точек.
5. Произносятся парольная фраза (при трехкратном повторении) для формирования шаблона TS (Template Speaker) (посредством преобразования набора признаков S_A, сформированном на основе конкатенации вектора признаков при верификации спикера по голосу, а также вектора признаков при распознавании слов фиксированной парольной фразы [6]).
6. Формируется нечеткий кодировщик GenS с помощью биометрического шаблона TS для скрытия k, при этом используется полиномиальное преобразование (p_2) и один из кодов исправления ошибок Cod_2.
7. Кодируется секретный ключ k с помощью GenS: k_{SS} = GenS(k, Cod_2, C_2), где C_2 – вспомогательная случайная последовательность.

Фаза проверки (верификации) инициализации

1. Вводится изображение отпечатка пальца TF′.
2. Формируется нечеткий экстрактор ExtF с помощью биометрического шаблона TF′ (посредством преобразования набора признаков F_B) для восстановления k, при этом используется полином p_1 и один из кодов исправления ошибок Cod_1.
3. Декодируется k' с помощью нечеткого экстрактора ExtF: k' = ExtF(k_{SF}, p_1, Cod_1).
4. Формируется хэш-образ извлеченного k': h(k').
5. Выполняется проверка равенства: h(k') == h(k)?.

Если равенство удовлетворяется, продолжение фазы проверки инициализации, иначе – выход по ошибке.

1. Произносится парольная фраза для формирования шаблона TS′ (посредством преобразования набора признаков S_B).
2. Формируется нечеткий экстрактор ExtS с помощью биометрического шаблона TS′ для восстановления k, при этом используется полиномиальное преобразование (p_2) и один из кодов исправления ошибок Cod_2.
3. Декодируется МК″ с помощью нечеткого экстрактора ExtS: k'' = ExtS(k_{SS}, p_2, Cod_2).
4. Формируется хэш-образ извлеченного k'': h(k'').
5. Выполняется проверка равенства: h(k'') == h(k)? Если равенство удовлетворяется, продолжение фазы проверки инициализации, иначе – выход по ошибке.
6. Зашифрование на мастер-ключе k критических параметров и данных, находящихся в секретной памяти (за исключением h(k)).
7. Удаление из секретной памяти k, а также из оперативной памяти: k', k'' и других оперативных критических данных.

Достоинствами предложенной схемы аутентификации являются следующие:

1. После фазы проверки инициализации в памяти устройства не сохраняется мастер-ключ и другие критические данные в открытом виде.
2. Фаза аутентификации пользователя на персональном устройстве преимущественно производится с помощью ввода изображения отпечатка пальца (шаги 1-5 фазы верификации, с возможным повтором не более трех раз).
3. В случае сбоя аутентификации на основе отпечатка пальца реализуется запасной вариант – аутентификация на основе парольной фразы. При успешном восстановлении мастер-ключа k, выполняется повторно этап инициализации (шаги 2-4) для восстановления работоспособности аутентификации на основе отпечатка пальца (возможно другого).
4. Для надежности функционирования системы восстановления (так называемой отменяемой биометрии), может быть задействован механизм периодической проверки работоспособности аутентификации на основе парольной фразы. Если данная верификация дает сбой, выполняется восстановление данного типа аутентификации посредством повторного прохождения этапа инициализации (шаги 5-7) (возможно с другой парольной фразой).
5. Для приложений с повышенными требованиями безопасности может быть реализован режим двухфакторной аутентификации (на основе отпечатка пальца и парольной фразы).

Список литературы

1. Ращеня Н.А. Портативный защищенный коммуникационный модуль / Н.А. Ращеня, Г.Ф. Астапенко, П.В. Кучинский, М.И. Новик // Приборостроение-2021: материалы 14-й Международной научно-технической конференции, 17-19 ноября 2021 года, Минск, Республика Беларусь / редкол.: О. К. Гусев (председатель) [и др.]. – Минск: БНТУ, 2021. – С. 118-120.
2. Skywire 4G LTE Cat 4 EU. Embedded Cellular Modem (datasheet). NimbeLink Corp, 2019, 24 P. Режим доступа: https://nimbelink.com/Documentation/Skywire/ 4G_LTE_Cat_4_Telit/1002044_NL-SW-LTE-TC4EU_Datasheet.pdf.
3. ZKTeco Fingerprint Scanners Hardware Selection Guide-v3.1. ZKTeco. Режим доступа: www.zkteco.com. – 2020.
4. Kumar N. Cancelable Biometrics: a comprehensive survey / Manisha and Nitin Kumar // Artificial Intelligence Review – 2020. – V. 53. – P. 3403-3446.
5. Mehmood R. Polynomial Based Fuzzy Vault Technique for Template Security in Fingerprint Biometrics / Reza Mehmood, Arvind Selwal // The International Arab Journal of Information Technology – 2020. – Vol. 17, No. 6. – P. 926-934.
6. Ращеня Н.А. Использование голоса (речи) для начальной и периодической верификации / Н.А. Ращеня, Г.Ф. Астапенко // Прикладные проблемы оптики, информатики, радиофизики и физики конденсированного состояния: материалы шестой Междунар. науч.-практ. конф. 20 – 21 мая 2021 г., Минск, М-во образования Респ. Беларусь, НИУ «Ин-т приклад. физ. проблем им. А.Н. Севченко Беларус. гос. ун-та. –2021. – С. 110-112.

УДК 004.056

МОНИТОРИНГ И УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ В АСУ ТП

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

Рассмотрим кратко, что есть объект исследования и каковы его технические (статистические) характеристики. Объектом исследований будем полагать системы АСУТП – автоматизированные системы управления технологическим процессом без определения узкой специализации применения по отраслям, архитектуре или составу компонентов. Далее рассмотрим данные статистики за последние три года.

В 2021 г. на объекты критической инфраструктуры (КИИ) компании Colonial Pipeline проведена достаточно показательная атака с использованием известных уязвимостей. Как отмечали эксперты команды Team82 из компании Claroty[4], более 90% уязвимостей достаточно легко эксплуатировать, а общий рост уязвимостей АСУТП превысил 40% по сравнению с 2020 г. Весьма опасно, что для 26% уязвимостей исправления отсутствуют, либо доступны только в виде частичных мер. Чаще всего уязвимости обнаруживаются в продуктах компании Siemens, Schneider Electric, Rockwell Automation, WAGO и Advantech. В 2020 г. обнаружено, что по сравнению с 2019 г. количество уязвимостей в АСУТП увеличилось на 10,3%. Более 75% уязвимостей были оценены как опасные (53,15%) или критические (22,47%) по шкале CVSS. Как отметили эксперты[5], более 70% уязвимостей можно эксплуатировать удаленно, а наиболее частым потенциальным воздействием было чтение данных приложений (41%), вызов отказа в обслуживании (39%) и обход механизмов защиты (37%). В 2019 г. опубликовано исследование[6] о неполной применимости общей системы оценки уязвимости (Common Vulnerability Scoring System, CVSS) для компонентов АСУТП, поскольку оценки нередко не соответствуют реальной степени опасности проблемы, что может повлечь за собой негативные последствия. Несмотря на то, что применение CVSS для оценки уязвимостей закреплено в различных стандартах, в том числе в PCI DSS, метрики CVSS не во всех случаях точно характеризуют уязвимости АСУТП. Отмечается, что в случае АСУТП более подходящей будет контекстная метрика, а наиважнейшим фактором должна быть доступность (что отмечено на примере уязвимости CVE-2015-5374, эксплуатируемой в атаках Industroyer / Crashoverride для вывода из строя реле Siemens).

Соответственно, краткий анализ статистики позволяет перейти к определению наиболее релевантных предметов исследований для объектов АСУТП:

1. быстрый рост уязвимостей в компонентах (двузначный рост в процентах);
2. возможности обхода механизмов защиты (двузначная доля в процентах);
3. неприменимость многих известных систем оценок.

---

[4] https://www.securitylab.ru/news/523530.php
[5] https://www.securitylab.ru/news/511354.php
[6] https://www.securitylab.ru/news/496586.php

В развитие данного промежуточного вывода можно отметить, что общая культура формирования проблемы обеспечения безопасности компонентов АСУТП пока недостаточно учитывает риски [1, 2]. Вообще «проникновение» практик риск-менеджмента в инженерную культуру нельзя полагать достаточной, поскольку наиболее известные в отрасли ИТ и ИБ стандарты ISO/IEC (ГОСТ Р ИСО/МЭК) серии 61508, 61511, 27001, 27005, 31000, 31010 и иные не в полной мере применяются в РФ в настоящее время. Из этого объективно следует еще один предмет исследования – применимость современных стандартов для оценивания компонент АСУТП [3, 4].

Часть 2. Текущее состояния объекта исследования

Специалисты признают[7], с некоторыми оговорками, что в АСУТП невозможно использовать такие же подходы, как при обеспечении ИБ в корпоративных сетях, но некоторые рекомендации хорошо применимы и для объектов АСУТП в рамках рассмотренных выше предметов исследований. В частности, можно отметить:

1. проведение аудита (что является обязательным требованием стандартов);
2. тестирования проектных решений на стенде (цифровом двойнике);
3. проведению периодических киберучений.

С учетом данных рекомендаций применительно к проблеме обеспечения соответствия (как более общего, включающего и аудит, и тестирование и иные способы оценивания) весьма важным по-прежнему является вопрос применимости встроенных механизмов функциональной безопасности, реализованных противоаварийной автоматической защитой (ПАЗ). Уполномоченный регулятор в РФ – ФСТЭК неоднократно утверждал, что наличие ПАЗ не является основанием для вывода о невозможности ущерба при компьютерном инциденте и не учитывается как мера защиты[8]. Следует отметить, что позиция ФСТЭК[9] о «недоверии» к компенсирующим (дублирующим) мерам предотвращения компьютерных инцидентов, не подверженных компьютерным атакам. (ПАЗ, предохранительные клапана и пр.) не имеет обоснования [5].

В качестве примера рассмотрим известный инцидент: вирус Triton, который был ориентирован на конкретный тип ПАЗ[10]. С учетом того, что ПАЗ поддерживает удаленное конфигурирование, именно на этот «транспорт» была направлена атака. Более того, сетевой протокол «транспорта» не предусматривал меры безопасности, хотя эти меры кибербезопасности были описаны еще в 2013 г. и аппаратный ключ котроллера ПАЗ находился в положении, позволявшем удаленно осуществлять конфигурирование. Этот пример подтверждает ранее показанный пример статистики, что около 37% уязвимостей реализуют вектор обхода механизмов защиты (37%). Таким образом, снова можно поднять вопрос о том, какая информация доступа в мире и в РФ из сети интернет. В качестве примера рассмотрим данные InfoWatch за 2021 г. (см. рис. 1)

К сожалению, приходится констатировать доступ даже к информации, отнесенной в установленном порядке к сведениям, составляющим государственную тайну. В РФ наблюдается ситуация, при которой доля публично доступной в сети интернет государственной тайны (6,7%) превышает, к сожалению, долю доступной коммерческой тайны (5,4%). Оче-

---

[7] https://www.securitylab.ru/analytics/527950.php

[8] https://www.securitylab.ru/blog/personal/valerykomarov/350544.php

[9] https://www.securitylab.ru/blog/personal/valerykomarov/350200.php

[10] https://www.securitylab.ru/blog/company/solarsecurity/347320.php

Рисунок 1. Информация, доступная из сети интернет (InfoWatch)

видно, эти данные отражают как несовершенство применяемых мер защиты, так и практику выявления и устранения уязвимостей в ведомственных информационных системах.

Часть 3. Существующие технологии и меры защиты

Рассмотрим далее, какую идеологию в области технологий и меры защиты нам готовы сегодня предложить ведущие мировые и российские поставщики.

В докладе «Актуальные вопросы повышения качества проектов и продуктов по ИБ» Е. Кожемяка («Конфидент») повторяет подход ФСТЭК о «накладных» мерах защиты, вводя еще одну проблему – устранение уязвимостей в сертифицированных решениях (см. рис. 2). К сожалению, не приводятся никакие оценки как именно дополнительные «накладные» меры защиты будут проходить сертификацию для конкретных условий функционирования компонентов АСУТП и изменение показателей обеспечения безопасности АСУТП в целом.

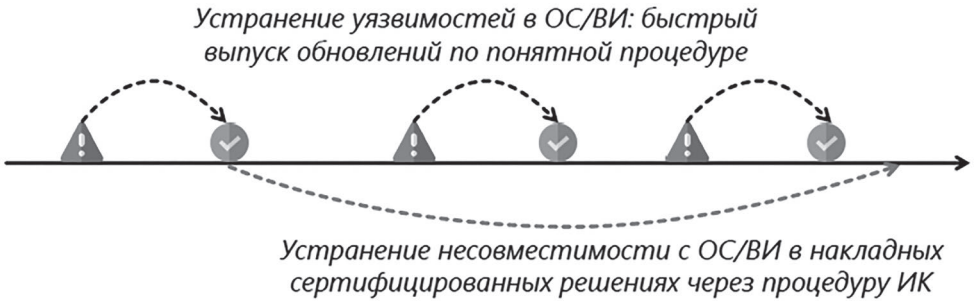


Рисунок 2. Устранение уязвимостей в «накладных» решениях («Конфидент»)

В докладе «Безопасная разработка и сертификация» Пономарева (ООО «НТЦ Фобос-НТ») отмечается, что многие нормативные документы в РФ не имеют статус обяза-

тельных и, наряду с рассмотренными выше стандартами ISO/IEC (ГОСТ Р ИСО/МЭК), весьма редко применяются. В частности, рассматривался ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения» и отмечалось, что этот национальный стандарт в РФ носит рекомендательный характер.

В докладе «От защиты АСУ ТП к безопасности предприятия» Даренского (Positive) приводится верный тезис: «в индустрии не существует IDS для 1С и никто не просит анализировать на трафике транзакции и платёжки». На практике вся совокупность финансовых транзакций (если верить сообщениям операторов «Диадок», «Тензор» и «Астрал» – это миллиарды документов в год) аккуратно контролируются компонентами ПО в точном соответствии с приказами ФНС, правил ПБУ и пр. Очевидно, что «разбирать» каждый план счетов и каждую транзакцию для каждой организации просто бессмысленно. В этой связи удобно продолжить этот тезис и задать вопрос – почему же АСУТП попадает в сферу бесконтрольного коммерческого интереса поставщиков «накладных» мер защиты, дающих якобы ««универсальный» эффект для всех типов информационных систем?

Часть 4. Предложения по мониторингу и управлению уязвимостями

Стандарт IEC 61508-1 определяет все необходимые термины для мониторинга и управления уязвимостями:

1. Safety Instrumented System (SIS) – автоматическая система функциональной безопасности, обеспечивающая применение одной или нескольких автоматических функций безопасности (Safety Instrumented Function, SIF). SIS предназначена для предотвращения или смягчения для объекта (устройства, объекта, оборудования, процесса) эффекта от наступления опасных событий путём его возвращения в функционально безопасное состояние в случае нарушения заданных условий его функционирования. В широком смысле примерами SIS-систем являются системы автоматической блокировки, системы аварийного отключения (Emergency ShutDown system, ESD), системы аварийного останова (Safety ShutDown system, SSD).
2. Safety Instrumented Function (SIF) определяется как автоматическая функция безопасности. SIF предназначена для предотвращения наступления или смягчения эффекта для объекта (устройства, объекта, оборудования, процесса) от опасного события посредством его возврата к приемлемому уровню риска. SIF имеет присвоенный ей Уровень полноты безопасности (Safety Integrity Level, SIL) в зависимости от величины риска, который должен быть уменьшен).
3. Safety Integrity Level (SIL) определяется как Уровень полноты безопасности. SIL является мерой эффективности SIS. Существуют 4 дискретных уровня целостности, связанных с понятием SIL. Чем выше уровень SIL, тем ниже вероятность отказа по запросу (PFD).
4. PFD (Probability of Failure on Demand) – вероятность отказа при запросе. Задает вероятность того, что система безопасности в случае необходимости не выполнит свою функцию.
5. PFDavg – Average Probability of Failure on Demand – средняя вероятность отказа функции при подаче запроса.
6. SFF – Safe Failure Fraction – доля неопасных отказов. Рассчитывается из отношения суммы неопасных отказов и диагностированных или распознанных отказов к полной интенсивности отказов системы.

Стандарт IEC 61508-1 явно различает два типа компонентов:

1. тип А — характеристика отказа определена полностью и отказы установлены;
2. тип В — компоненты с неопределенной характеристикой отказа по крайней мере одного элемента, например, для микропроцессоров.

Учет типа компонента позволяет точно определить соответствующий SIL для компонента АСУТП. Логично предположить, что этот же подход должен быть применён при оценивании всех компонентов АСУТП, в том числе рекомендуемых «наложенных» средств. С учётом того, что производители не приводят реальных данных по быстродействию и/или надежности своих объектов, уместно предположить, что все они имеют в своём составе как минимум 1 компонент типа В и должны проходить оценку по тем же критериям, что и компоненты АСУТП [4, 5]. Иначе в равнопрочном поле безопасности возникают неконтролируемые и неоцененные с точки зрения безопасности области «накладных» мер защиты, в отношении которых не представлены никакие объективные свидетельства соответствия установленным требованиям в области безопасности.

Рассмотрим примеры компонентов АСУТП, которые прошли в установленном порядке оценивание по требованиям стандарта IEC 61508 и имеют сертификат SIL:

1. Технологическое оборудование компании «Астутек»[11];
2. Компоненты систем технологической автоматики[12];
3. Электронные компоненты АО «Вика Мера»[13];
4. Системы вентиляции, насосы, отопительные системы[14];
5. Компоненты систем управления[15];
6. Системы обеспечения безопасности Siemens[16].

Важно обратить внимание, что полученный при независимой сертификации уровень полноты безопасности SIL дает и поставщику и владельцу объекта КИИ широкий диапазон допустимых вариантов обеспечения безопасности. Известно, что SIL 4 является самым высоким уровнем снижения риска, который может быть достигнут посредством применения SIS. Но эксперты[17] полагают, что достижение уровня SIL 4 не всегда является реалистичным, и в настоящее время существует малое число систем, которые поддерживают этот уровень (как правило, по причине исключительно высокой стоимости). В тоже время, если «защищаемый» процесс на объекте КИИ несёт в себе такие высокие риски, что требуется система уровня SIL 4 для приведения его в безопасное состояние, то в большинстве случаев проблему решают путем изменения процесса или применения других (не автоматических) методов снижения рисков. Например, в соответствии с требованиями стандарта IEC (ГОСТ Р МЭК) 31010, определено более 40 методов обработки (снижения) рисков, которые достаточно давно известны и широко представлены в индустрии – например, FMEA, FTA, HAZOP и пр.

---

[11] https://astutek.ru/blog/item/sil-sil-1-sil-2-i-sil-3-oborudovanie-s-markirovkoj-sil

[12] http://efomation.ru/products/oborudovanie-zashchiti/standarti-sil.html?

[13] https://www.wika.ru/upload/DS_IN0019_ru_ru_73327.pdf?ysclid=l27ne68d8b

[14] https://www.heatingandprocess.com/sil3/

[15] https://www.cta.ru/cms/f/428100.pdf

[16] https://controlengrussia.com/sistemy-avarijnoj-zashhity/safety_instrumented_system/?

[17] http://www.kconsult-cis.com/news/2015/11/06/23.html

Часть 5. Выводы

1. Для обеспечения безопасности АСУТП предлагается прекратить искусственное разделение «видов безопасности» ИТ, ИБ и функциональной безопасности. Очевидно, что попытки «латания» уязвимостей «наложенными» средствами защиты, не затрагивая архитектуры, процессы безопасного проектирования, аудита и тестирования, не приведут к успеху.
2. Настоятельно рекомендуется применение риск-ориентированных стандартов и имеющейся экспертизы для компонентов АСУТП, полностью уйти от фиксированных моделей угроз и применения «наложенных» мер с неизвестным качеством и неоцененным уровнем безопасности.
3. Предоставить разработчикам компонентов АСУТП возможности независимой оценки соответствия (сертификации) по требованиям признанных международных (ISO/IEC) и национальных (ГОСТ Р) стандартов для обеспечения объективной и непредвзятой оценки уровня безопасности объектов КИИ.

Список литературы

1. Livshitz I.I., Neklyudov A.V., Lontsikh P.A. IT security evaluation — “hybryd” approach and risk of its implementation // Journal of Physics: Conference Series. 2018. V. 1015. N 4. P. 042030. doi: 10.1088/1742-6596/1015/4/042030
2. Лившиц И.И. Практика управления киберрисками в нефтегазовых проектах компаний холдингового типа // Вопросы кибербезопасности. 2020. №1(35). С. 42–51. doi: 10.21681/2311-3456-2020-01-42-51
3. Лившиц И.И., Неклюдов А.В. Методика оптимизации программы аудитов информационной безопасности // Комплексная защита информации: материалы XXII научно-практической конференции. Новополоцк: Полоцкий государственный университет, 2017. С. 135–139.
4. Лившиц И.И. Метод оценивания безопасности облачных ИТ- компонент по критериям существующих стандартов // Труды СПИИРАН. 2020. Т. 19. № 2. С.383–411. doi: 10.15622/sp.2020.19.2.6
5. Лившиц И.И. К вопросу обеспечения безопасности промышленных систем // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, №1. С. 1–14. doi: 10.17586/2226-1494-2021-21-1-1-14

УДК 621.38

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ И ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ МИКРОЭЛЕКТРОННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ НОРМАТИВНЫХ ДОКУМЕНТОВ

К.А. БОЧКОВ, С.Н. ХАРЛАП, П.М. БУЙ
Белорусский государственный университет транспорта,
г. Гомель, 246653, Республика Беларусь

Информационная и функциональная безопасность

На современном этапе развития информационных технологий, активным внедрением этих технологий в различные сферы экономики и промышленности, вопросы информационной безопасности становятся все более актуальными и их значение все более возрастает. Особенно это заметно в моменты обострения мировой политической обстановки, когда обеспечение информационной безопасности становится жизненно необходимым для выживания государства. В последнее время актуальными стали вопросы защиты объектов информационной инфраструктуры от кибератак и кибертерроризма.

Кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации [1].

Кибертерроризм – атаки на информационные системы, несущие угрозу здоровью и жизни людей, а также способные спровоцировать серьезные нарушения функционирования критически важных объектов в целях оказания воздействия на принятие решений органами власти, либо воспрепятствования политической или иной общественной деятельности, либо устрашения населения, либо дестабилизации общественного порядка [1].

Однако следует учитывать, что объектами критической информационной инфраструктуры (КИИ), к которым предъявляются требования информационной безопасности, являются системы, которые очень сильно отличаются друг от друга в части требований условий функционирования, надежности и готовности, коммуникаций и т.д. А многообразие объектов КИИ требует в ответ многообразия методов обеспечения информационной безопасности, а так же признания того, что одни и те же методы будут иметь различную эффективность при их применении к различным объектам КИИ.

При этом безопасность людей, социальной и экологической сферы не является предметом информационной защиты. Методы и средства обеспечивающие исключительно информационную безопасность не в силах решить эти задачи. Особенно это актуально для автоматизированных систем управления ответственными технологическими процессами (АСУ ОТП), которые широко применяются в том числе на железнодорожном транспорте.

Далее мы остановимся на одном типе объектов КИИ, а именно автоматизированных системах управления на транспорте, а точнее системах железнодорожной автоматики и телемеханики (ЖАТ). Особенностью систем ЖАТ является то, что в первую очередь данные системы должны выполнять требования функциональной безопасности, заключающиеся в

обеспечении безопасности движения поездов, и только во вторую очередь все остальные требования, включая требования информационной безопасности. Такой подход отражен в Приказе №31 ФСТЭК России от 14.0-3.2014 и Приказе №239 ФСТЭК России от 25.12.2017.

На протяжении уже более 200 лет разрабатывались и успешно применялись различные подходы, принципы и методы обеспечения функциональной безопасности, многие из которых не зависят от используемой элементной базы. Накопленные знания в области построения безопасных систем ЖАТ на текущем этапе развития могут успешно применяться и для решения новых задач, связанных с нарушением информационной безопасности.

Функциональная безопасность (functional safety) системы управления – это часть общей безопасности системы, работающей правильно в ответ на входные воздействия и обеспечивающей отсутствие неприемлемого риска здоровью людей, их собственности или окружающей среде со своей стороны [2]. Т.е. система, отвечающая требованиям функциональной безопасности, не должна подвергать опасности здоровье и жизнь людей, приводить в значительным экономическим потерям и разрушению окружающей среды.

Основополагающим стандартом верхнего уровня в области функциональной безопасности стал IEC 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью». В Российской Федерации от известен как ГОСТ Р МЭК 61508-2012. Это фундаментальный стандарт в семи частях содержит не только требования к системам АСУ ТП, но и основные методы для достижения выполнения этих требований. Этот же стандарт ранжирует системы, связанные с безопасностью, по уровню полноты безопасности (УПБ), который может быть определен как количественно через интенсивность или вероятность опасного события, так и качественно через величину возможного ущерба. Положения этого стандарта детализированы в соответствующих отраслевых стандартах. Системы ЖАТ по данной классификации относятся к наивысшему четвертому уровню полноты безопасности УПБ4.

В последних поколениях систем ЖАТ, построенных с использованием аппаратно-программных комплексов на базе локальных и внешних сетей связи с автоматизированными рабочими местами операторов и центрами управлением движением поездов естественным образом возникает проблема обеспечения информационной безопасности. На сегодня проблема информационной безопасности систем ЖАТ решается следующим образом. Разработчик сначала должен выполнить все установленные процедуры по подтверждению соответствия требованиям функциональной безопасности (испытаний, верификации ПО и т.д.) и экспертизу специального документа «Доказательство безопасности» в соответствующей лаборатории, аккредитованной в области функциональной безопасности. Далее он должен выполнить ряд процедур подтверждения соответствия требованиям информационной безопасности с участием лаборатории, аккредитованной в области информационной безопасности. Результатом выполнения таких процедур является создание дополнительных средств защиты, которые являются внешними по отношению к средствам обеспечения функциональной безопасности.

Такой подход является избыточным, так как методы защиты частично могут дублировать друг друга. И хотя в Приказе №239 ФСТЭК России от 25.12.2017 рекомендовано, что если меры функциональной безопасности являются достаточными для нейтрализации актуальных угроз информационной безопасности, то дополнительные меры защиты можно не применять, эти рекомендации на практике не выполняются. Основанием для этого служат различия в перечне угроз и объектов защиты. Интегрировать же дополнительные средства защиты в комплекс мер функциональной безопасности невозможно, т.к. это по-

требует повторной процедуры подтверждения соответствия требованиям функциональной безопасности.

Кроме того, следует отметить, что законодательство Республики Беларусь не определяет область обеспечения функциональной безопасности, процессы ее взаимодействия с информационной безопасностью, методы организации и какие-либо требования к ней. Все вопросы обеспечения кибербезопасности включают в себя исключительно информационную безопасность, а зачастую именно так и называются.

Практический опыт испытаний и экспертиз различных систем ЖАТ позволяет сделать вывод о том, что методы обеспечения функциональной безопасности и информационной безопасности достаточно близки и могут быть интегрированы на ранних этапах разработки. При этом приоритет должен отдаваться методам обеспечения функциональной безопасности и решению с их помощью задач информационной безопасности.

Стратегии обеспечения функциональной безопасности

Для обеспечения функциональной безопасности используются несколько подходов (стратегий): безотказность, отказоустойчивость и безопасное поведение при отказах [3]. В первом случае предлагается использовать высоконадежные элементы, во втором – использовать различные методы резервирования и восстановления для обеспечения отказоустойчивости. Т.е. первые две стратегии направлены на общее повышение надежности (безотказности), и как следствие повышение безопасности за счет сохранения работоспособности системы и обеспечение ее правильной работы в различных ситуациях, в том числе ее устойчивости при воздействии внешних факторов. Однако такой подход ограничен надежностью используемой элементной базы и может использоваться при построении систем с уровнем полноты безопасности не превышающем УПБ3. Для систем с УПБ4 такой подход не обеспечивает выполнение требований функциональной безопасности.

Третья стратегия является специфичной для систем ЖАТ и предполагает разделение неработоспособного состояния системы на два состояния: неработоспособное защитное (безопасное) и неработоспособное опасное. Для этой цели все функции, выполняемые системой, делятся на два класса: технологические функции, не связанные с обеспечением безопасности, и функции обеспечения безопасности. Если часть технологических функций по каким-либо причинам не может быть выполнена, но при этом все функции обеспечения безопасности выполняются в полном объеме, то система находится в защитном (безопасном) состоянии. При невыполнении хотя бы одной функции обеспечения безопасности система переходит в опасное состояние. Соответственно различают опасные и защитные отказы.

Опасный отказ системы ЖАТ может привести к возникновению аварии или крушению поезда, но в подавляющем большинстве случаев этого не происходит, поскольку причины возникновения аварии (крушения) связаны также с существующей в данный момент поездной ситуацией и действиями человека-оператора (машинист, дежурный по станции, поездной диспетчер, электромеханик и др.)

Вероятность возникновения аварии (крушения) при этом определяется выражением:

$$Q_A = Q_{оп} \cdot Q_{пс} \cdot Q_{чо}\ , \qquad (1)$$

где $Q_{оп}$ – вероятность опасного отказа системы ЖАТ; $Q_{пс}$ – вероятность существования аварийной поездной ситуации; $Q_{чо}$ – вероятность невыполнения человеком-оператором действий по предотвращению (парированию) аварии (крушения).

Исходя из этого, отказ системы ЖАТ считается опасным, если нарушен критерий опасного отказа, даже если авария (крушение) при этом не произошла. Это позволяет рассматривать безопасность системы или отдельного её элемента как свойство объекта вне связи с ошибками человека или движением поездов. Диаграммы состояний объекта СЖАТ можно представить в виде

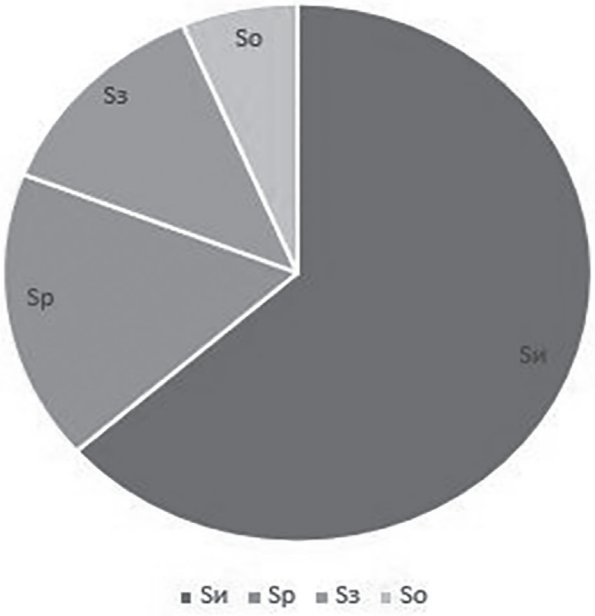


Рисунок 1. Диаграмма состояний объекта СЖАТ

где $S_И$, $S_Р$, $S_З$, $S_О$ – подмножества исправных, работоспособных, защитных и опасных состояний.

Безопасность системы ЖАТ при этом определяется, как свойство системы непрерывно сохранять исправное, работоспособное или защитное состояние в течении некоторого времени или наработки.

Защитный отказ нарушает безотказность, но не нарушает безопасность. Опасный отказ нарушает и безотказность, и безопасность.

Безотказность характеризуется множеством состояний

$S_Н = S_И \cup S_Р$,

а безопасность – множеством состояний

$S_Б = S_И \cup S_Р \cup S_З$.

Критерии опасных отказов в обязательном порядке устанавливаются в соответствующей нормативной документации. Такой подход позволяет сконцентрироваться на относительно небольшом множестве функций и критических элементов и использовать достаточно сложные методы защиты.

Иерархия уровней защиты

Многообразие отказов и форм их проявления требует применения методов обеспечения безотказности и безопасности на различных функциональных уровнях микроэлектронных систем ЖАТ. На сегодняшний день наиболее перспективным для управления рисками счи-

тается принцип «Защита в глубину» (Defense-in-Depth), который заключается в том, что в системе должен применяться набор разнотипных методов защиты, с тем, чтобы инцидент либо авария на объекте контроля и управления не мог пройти все уровни. Обычно выделяют пять уровней защиты: аппаратный (самый низкий), информационный, программный, структурный и уровень интерфейса (самый высокий) [4].

Такая иерархия обусловлена тем, что на каждом из этих уровней можно осуществлять мероприятия по защите от отказов, позволяющие компенсировать последствия отказов, возникающих на более низких уровнях. Например, использование на структурном уровне диверситетного программного обеспечения позволяет защититься от ошибок в программном обеспечении, использование парафазного кодирования на информационном уровне позволяет контролировать исправную работу самопроверяемых схем.

На практике, далеко не всегда защита осуществляется на всех уровнях одновременно. Обязательным является применение структурных методов обеспечения безопасности и безопасного интерфейса с исполнительными объектами, то есть высших уровней защиты. Мероприятия по защите от опасных отказов на остальных уровнях применяются при необходимости повышения показателей функциональной безопасности.

На каждом из уровней защиты от опасных отказов могут использоваться различные подходы и стратегии обеспечения безопасности. Например, на информационном и программном уровнях наиболее часто применяют стратегию отказоустойчивости, а на аппаратном, структурном и уровне интерфейса – стратегию безопасного поведения при отказах. Кроме того, на одном уровне защиты могут использоваться несколько различных стратегий одновременно. Например, стратегия безопасного поведения может применяться совместно со стратегией отказоустойчивости. В этом случае, если при возникновении отказов система исчерпала резервные возможности и в результате деградации и реконфигурации перестала быть отказоустойчивой, то при появлении еще одного отказа она должна необратимо перейти в защитное состояние.

Такой подход обеспечивает многообразие путей решения проблемы обеспечения заданных показателей безопасности, но окончательный выбор всегда остается за разработчиком системы.

Методы обеспечения функциональной безопасности

Для того, чтобы сравнить эффективность применения методов функциональной безопасности для решения задач информационной безопасности необходимо рассмотреть следующие элементы: поставленные цели, последствия (величина ущерба), объект защиты, угрозы безопасности.

В соответствии с Приказом №31 ФСТЭК России от 14.03.2014 целью мер по обеспечению информационной безопасности в первую очередь является обеспечение доступности и целостности обрабатываемой в АСУ ТП информации. Таким образом внимание концентрируется на защите информации с целью недопущения ее искажения (в том числе недоступности актуальной информации), которое может привести к нарушению функционирования АСУ ТП. Цели функциональной безопасности заключаются в отсутствии неприемлемого риска здоровью людей, их собственности или окружающей среде со стороны АСУ ТП при нарушении ее правильного функционирования. Очевидно, что цели функциональной безопасности шире, так как в качестве причин нарушения функционирования АСУ ТП учитываются не только возможные искажения информации, но и отказы аппаратных средств, ошибки в программном обеспечении и др.

Если внимательно посмотреть на критерии значимости объектов КИИ и сравнить их критериями ранжирования систем управления по функциональной безопасности, то можно сделать вывод, что требования функциональной безопасности гораздо жёстче, чем требования информационной безопасности. Так, например, ГОСТ 33433-2015 «Безопасность функциональная. Управление рисками на железнодорожном транспорте», устанавливающий типовые уровни тяжести последствий, относит к наивысшему, катастрофическому уровню последствий, аварийную ситуацию, повлекшую гибель одного или более людей. В то время как согласно Перечня показателей критериев значимости объектов критической информационной инфраструктуры, утвержденного Постановлением Правительства РФ от 8 февраля 2018 № 127, если инцидент на объекте КИИ приведет к гибели от одного до пятидесяти человек, то такой объект относят к низшей третьей категории.

Объектами защиты в АСУ ТП как с точки зрения информационной безопасности, так и с точки зрения функциональной безопасности являются:

- технические средства;
- программное обеспечение;
- информация о параметрах или состоянии управляемого объекта или процесса.

Однако при рассмотрении вопросов информационной безопасности концентрируют внимание на доступности и целостности информации, а технические средства и программное обеспечение рассматривают только как источники возможного искажения информации, временной недоступности или несанкционированного доступа к информации. При реализации мер по обеспечению функциональной безопасности в равной мере уделяют внимание как последствиям отказов технических средств, так и возможным ошибкам в программном обеспечении, в том числе приводящих к искажению критической информации.

Исходя из вышесказанного можно сделать вывод о том, что 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.

Угрозы информационной и функциональной безопасности

Типичными угрозами информационной безопасности являются события, связанные с нарушением доступности и целостности обрабатываемой в АСУ ТП информации, а именно [5-6]:

1. Внешние угрозы:
   - несанкционированный доступ;
   - саботаж или намеренное причинение ущерба сторонними лицами;
   - вредоносное ПО (вирусы);
   - целевые атаки.
2. Внутренние угрозы:
   - ошибки конфигурации оборудования;
   - саботаж или намеренное причинение ущерба сотрудниками;
   - уязвимости в индустриальном ПО и протоколах, том числе недекларированные возможности.

Типичными угрозами функциональной безопасности являются [4]:

1. Внешние угрозы:
   - случайные искажения информации в каналах связи;
   - отказы внешней инфраструктуры.

2. Внутренние угрозы:
   - отказы оборудования;
   - случайные искажения внутренней информации;
   - ошибки персонала (непреднамеренные действия);
   - ошибки в программном обеспечении.

Сравнение типичных угроз информационной и функциональной безопасности позволяет сделать следующий вывод. Методы функциональной безопасности направлены в первую очередь на защиту от случайных событий (неумышленных действий), в то время как информационная безопасность сконцентрирована на защите от умышленных (преднамеренных) действий злоумышленников. В этом и заключается основное отличие в подходах. На первый взгляд это требует применения принципиально разных подходов, но более глубокий анализ показывает, что это далеко не так.

Обеспечение доступности и целостности информации методами функциональной безопасности

Рассмотрим более подробно угрозы информационной безопасности применительно к основной цели – обеспечении доступности и целостности информации.

Доступность – это обеспечение своевременного и надежного доступа к информации и информационным сервисам.

Целостность – это отсутствие неправомочных искажений, добавлений или уничтожения информации.

Все рассмотренные выше угрозы при некоторых условиях могут нарушить доступность информации. При этом АСУ ТП перестанет получать актуальную информацию о состоянии объектов управления и контроля, что может стать потенциально опасным. Однако к таким последствиям могут привести также и случайные события, которые в обязательном порядке учитываются при разработке АСУ ТП в рамках обеспечения функциональной безопасности. Например, информация с рельсовых цепей участка железной дороги позволяет системе ЖАТ определить местоположения поезда и, в соответствии с этой информацией, включить соответствующую сигнализацию на проходных светофорах.

Парирование последствий нарушения доступности информации можно выполнять по двум направлениям:

1. сохранение доступности информации. В этом случае решение сводится к задаче повышения надежности системы, которая решается резервированием;
2. сохранение безопасного состояния системы при отсутствии доступа к критической информации. В этом случае могут быть использованы методы функциональной безопасности, которые, например, применяются в системах обеспечения безопасности при обрыве линии связи с источником ответственной информации.

В этом случае выполняется ряд мероприятий, позволяющих исключить возникновение опасной ситуации:

- ограничение времени жизни (актуальности) критической информации. Если информация не обновилась за указанный период времени, то она автоматически заменяется на более безопасное значения. Например, для рельсовой цепи при потере связи принимается, что контролируемый участок пути занят поездом;
- ограничение времени жизни команд. Бистабильные команды, которые вызывают переключение объекта (например, команды включить / выключить лампу светофора) име-

ют ограниченное время жизни. Если время жизни команды истекло, то объект автоматически переключается в защитное состояние;

- контроль последовательности выполнения процедур в программном обеспечении, который гарантирует что процедуры проверки актуальности информации / команд будут выполнены за указанный интервал времени;
- программный и аппаратный контроль тайм-аутов, исключающий сохранение активного состояния выходов в случае зависания вычислительных каналов.

Такая многоуровневая защита позволяет гарантировать переход в защитное состояние АСУ ТП при любых нарушениях доступности критической информации. Таким образом можно сделать вывод, что методы обеспечения функциональной безопасности позволяют в полной мере решить задачи информационной безопасности по обеспечению доступности информации в АСУ ТП в том объеме, который позволит исключить опасное влияние таких угроз на работу АСУ ТП.

Нарушение целостности данных тоже нужно рассматривать по нескольким направлениям:

- случайное (непреднамеренное) искажение информации (в том числе конфигурационной);
- преднамеренное искажение информации посредством внешних систем передачи информации. Сюда можно отнести такие угрозы как несанкционированный доступ, вредоносное ПО, целевые атаки, уязвимости в протоколах передачи данных;
- преднамеренное искажение информации посредством использования уязвимостей в ПО, в том числе недекларированных возможностей.

Случайное нарушение целостности информации (искажения, добавления или удаления) являются предметом функциональной безопасности. Концепция обеспечения безопасности, принятая разработчиками, должна исключать опасное влияние таких нарушений на безопасность системы в целом. Для этих целей разработан и успешно применяется ряд методов, таких как избыточное кодирование, дублирование с последующим сравнением, диверсификация способов кодирования и форматов хранения информации, защита с помощью контрольных сумм и т.д.

Защита систем ЖАТ от преднамеренного нарушения целостности информации через внешние системы передачи информации осуществляется в соответствии с ГОСТ Р МЭК 62280 «Железные дороги. Системы связи, сигнализации и обработки данных. Требования к обеспечению безопасной передачи информации». В данном стандарте рассмотрены возможные угрозы нарушения целостности данных, такие как случайные отказы аппаратных средств, систематические отказы (ошибки) программного обеспечения, внешние физические воздействия и преднамеренные действия злоумышленника. Выделены основные типы нарушения целостности: повтор, удаление, вставка, переупорядочивание, повреждение (искажение), задержка и подмена сообщений.

В стандарте также определены необходимые меры для защиты от опасных последствий этих нарушений: использование меток времени в сообщениях, избыточных кодов и криптографических методов. Рассмотренные в стандарте угрозы и меры защиты охватывают все возможные угрозы информационной безопасности и являются достаточными для их нейтрализации.

Защита систем ЖАТ от систематических отказов (ошибок) программного обеспечения осуществляется в соответствии с ГОСТ Р МЭК 62279 «Железные дороги. Системы связи, сигнализации и обработки данных. Программное обеспечение систем управления и защиты на железных дорогах». Стандарт охватывает все этапы жизненного цикла программно-

го обеспечения и регламентирует порядок разработки, документирования, верификации и внесения изменений в программное обеспечение. Рассмотрены вопросы организации разработки ПО, определены типовые роли, их компетенции, возможность совмещения разных ролей одним человеком. Рекомендован независимый аудит аккредитованной лабораторией на всех стадиях разработки, позволяющий обнаруживать ошибки на ранних этапах жизненного цикла.

В стандарте приведены методы, позволяющие получить программное обеспечение, соответствующее требованиям функциональной безопасности с УПБ4. Например, при разработке архитектуры ПО стандартом рекомендовано применять следующий набор методов: защищенное программирование, многовариантное (диверситетное) программирование, полностью определенный интерфейс, структурная методология, а также один из следующих методов: коды с обнаружением ошибок, программирование с проверкой ошибок, сохранение достигнутых состояний или моделирование.

Статический анализ кода, который является обязательным элементов верификации ПО, позволяет контролировать не только корректную реализацию спецификации, но и убедиться в отсутствии недекларируемых возможностей.

Выполнение всех мероприятий по защите от систематических отказов по ГОСТ Р МЭК 62279 позволяет получить программное обеспечение, соответствующее не только требованиям функциональной безопасности, но и требованиям информационной безопасности.

Этапы жизненного цикла, связанные с функциональной и информационной безопасностью

Структура жизненного цикла определена стандартами по функциональной безопасности [7], которые рекомендуют использовать V-образный жизненный цикл. По нисходящей ветви жизненного цикла выполняется разработка системы, а по восходящей ветви – интеграция, сопровождаемая процедурами верификации и валидации на соответствие требованиям. Этапы жизненного цикла объекта железнодорожного транспорта представлены на рисунке 2.

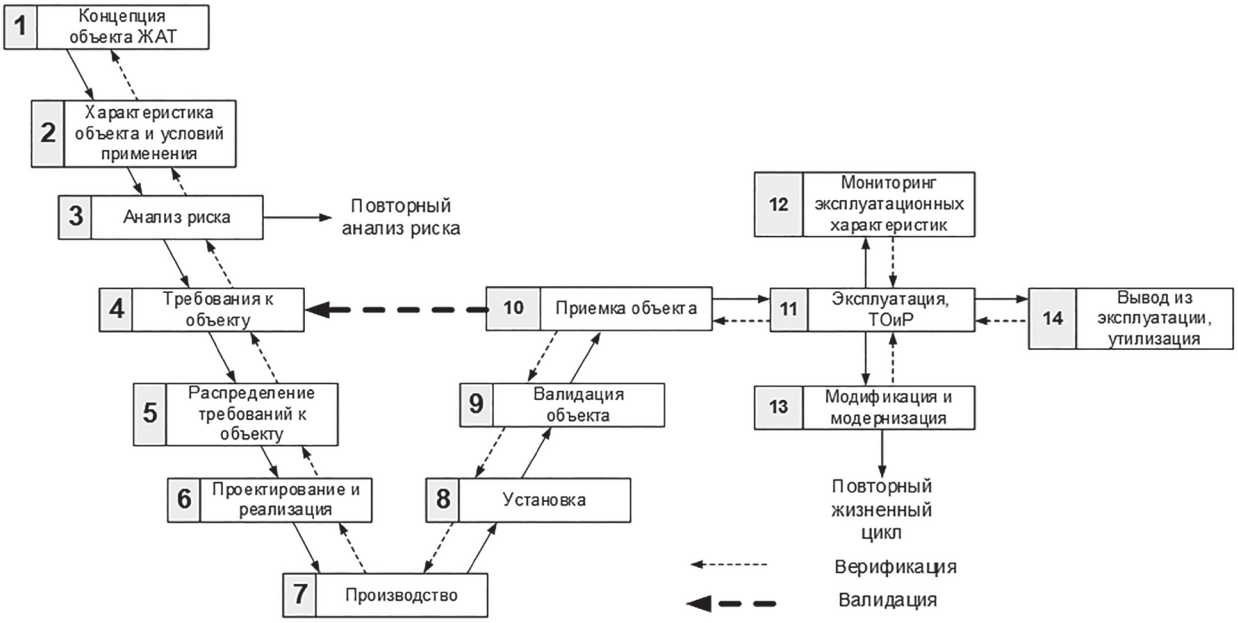


Рисунок 2. Этапы жизненного цикла объекта железнодорожного транспорта

Задачи, связанные с обеспечение информационной безопасности, можно интегрировать в жизненный цикл функциональной безопасности на ранних этапах разработки. Подробное описание такого подхода с перечнем задач функциональной и информационной безопасности, решаемых на каждом этапе жизненного цикла приведено в [8].

Отдельно отметим, что до этапа проектирования и реализации должны быть решены следующие задачи информационной безопасности:

- на этапе концепции объекта ЖАТ необходимо определить объекты защиты (технические средства, программное обеспечение, технологическая информация), документировать потенциальные внутренние и внешние угрозы функциональной и информационной безопасности. Выявить общие объекты защиты и угрозы безопасности. Составить общий перечень угроз безопасности, в котором угрозы функциональной безопасности должны быть дополнены угрозами информационной безопасности;
- на этапе «Характеристика объекта ЖАТ и условий его применения» необходимо разработать Программу обеспечения функциональной безопасности [7] и Программу информационной безопасности. При этом Программу информационной безопасности можно интегрировать в Программу обеспечения функциональной безопасности, использовав одинаковые методы для защиты от общих угроз безопасности, и добавив специальные методы для защиты от специфичных угроз информационной безопасности;
- на этапе анализа рисков выполнить идентификацию опасностей как с точки зрения функциональной, так и информационной безопасности. Для каждой опасности определить уровень риска и разработать мероприятия по снижению риска. На этом этапе также удобно интегрировать работы по информационной безопасности в мероприятия по реализации функциональной безопасности;
- на этапах «Требования к объекту ЖАТ» и «Распределение требований к объекту ЖАТ» определяются общие требования надежности, функциональной и информационной безопасности, а также общие критерии доказательства и подтверждения соответствия требованиям функциональной и информационной безопасности.

На этих этапах разработчик должен привлекать специалистов как в области функциональной, так и в области информационной безопасности.

При таком подходе при проектировании и реализации объекта ЖАТ будут в равной мере учтены как требования функциональной, так и требования информационной безопасности. Разработчик сможет применять наиболее эффективные методы на различных уровнях защиты, что позволит не только повысить уровень защищенности системы от выявленных опасностей, но и исключить дублирование средств защиты.

На этапах жизненного цикла, связанных с валидацией и приемкой объекта, возникает задача подтверждения соответствия требованиям функциональной и информационной безопасности. Учитывая глубокую интеграцию методов защиты, реализованной на ранних этапах жизненного цикла, такие работы желательно проводить в одной испытательной лаборатории, аккредитованной как в области функциональной, так и в области информационной безопасности.

Выводы

Использование методов функциональной безопасности позволяет в полном объеме решить задачи информационной безопасности для АСУ ТП. Для всех угроз информационной

безопасности существуют эффективные методы защиты, базирующиеся на стандартах по функциональной безопасности.

Для эффективного использования методов функциональной безопасности в целях обеспечения информационной безопасности необходимо выполнять эту работу на ранних стадиях разработки АСУ ТП, начиная с технического задания. При этом для исключения дублирования работ подтверждение соответствия требованиям функциональной и информационной безопасности желательно проводить в одной организации, аккредитованной в этих областях.

Список литературы

1. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета безопасности Респ. Беларусь, 18 марта 2019 г., № 1 // ЭТАЛОН Online. Законодательство Республики Беларусь / Нац. центр правовой информации Респ. Беларусь. – Минск, 2019.
2. ГОСТ Р МЭК 61508-4-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения. – Москва: Стандартинформ, 2014 – 28 с.
3. 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.
4. Харлап, С. Н. Применение диверситета в автоматизированных системах управления опасными технологическими процессами для повышения устойчивости к систематическим отказам / С. Н. Харлап // Известия Транссиба. – 2020. – № 3 (43). – С. 148 – 157.
5. Надеждин, Ю. Безопасность АСУ ТП критически важных объектов // http://lib.secuteck.ru/articles2/security-director/bezopasnost-asu-tp-kriticheski-vazhnyh-obektov. – Дата доступа: 19.04.2022.
6. Мальнев, А. Противодействие реальным угрозам АСУ ТП // Information Security/ Информационная безопасность. – 2015. – №4.
7. ГОСТ 33432-2015. Безопасность функциональная. Политика, Программа обеспечения безопасности. Доказательство безопасности объектов железнодорожного транспорта. – Москва: Стандартинформ, 2016 – 22 с.
8. Скляр В. В. Обеспечение безопасности АСУ ТП в соответствии с современными стандартами: Методическое пособие. / В. В. Скляр. – М.: ИнфраИнженерия, 2018. – 384 с.

ПОДГОТОВКА КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

НОВЫЙ ПЕРЕЧЕНЬ СПЕЦИАЛЬНОСТЕЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – 2024, ПОДХОДЫ К РАЗРАБОТКЕ МАКЕТА ФГОС – 4.

БЕЛОВ Е.Б.

Заместитель председателя Федерального УМО
в системе высшего образования по УГСНП 10.00.00 «Информационная безопасность»

Подготовка кадров в области информационной безопасности (далее – ИБ) имеет существенные особенности, поскольку выступает не только как реакция на спрос рынка труда и в целом цифровой экономики России в отношении таких специалистов, но и как важная составляющая комплекса мероприятий государства по противодействию угрозам в информационной сфере. Этими особенностями определяются и содержание подготовки соответствующих специалистов, и особые требования, предъявляемые к образовательным организациям при реализации такой подготовки. Указанные особенности нашли свое отражение в принципах формирования нового Перечня направлений подготовки и специальностей для области «Информационная безопасность».

«Научные подходы и принципы формирования нового перечня направлений и специальностей в области «Информационная безопасность»

Для УГСНП:

- полный охват направлениями подготовки и специальностями предметной области «Информационная безопасность»;
- соответствие профессиональным стандартам (далее – ПС) по группе занятий (профессий) «Специалисты в области информационной безопасности»;
- соответствие современным и перспективным направлениям развития индустрии «Информационная безопасность». Наличие в национальной программе «Цифровая экономика Российской Федерации» федерального проекта «Информационная безопасность» блока мероприятий кадрового обеспечения в данной сфере (утв. правительственной комиссией, протокол от 27 декабря 2018 г. № 6);
- соответствие Стратегии научно-технологического развития Российской Федерации на долгосрочный период;
- учет требований уполномоченных федеральных органов исполнительной власти, ответственных за обеспечение ИБ, к уровню подготовки специалистов;
- постоянный рост объема контрольных цифр приема (далее – КЦП) для УГСНП 10.00.00 «Информационная безопасность».

Для направлений подготовки:

- полный охват направлениями (интегрированным направлением) подготовки предметной области «Информационная безопасность»;
- соответствие профессиональным стандартам по группе занятий (профессий) «Специалисты в области информационной безопасности»;

- объединение направлений, имеющих общую фундаментальную подготовку, с возможностью их дальнейшей профилизации;
- объединение направлений, имеющих общую прикладную (отраслевую) ориентацию подготовки.

Для специальностей:

- направленность содержания подготовки специалистов на реализацию системных подходов к обеспечению безопасности личности, общества, государства;
- соответствие профессиональным стандартам по группе занятий (профессий) «Специалисты в области информационной безопасности» (соответствие каждой специальности ключевому однородному профессиональному стандарту (профессиональным стандартам);
- учет требований основных потребителей (заказчиков) к квалификации выпускника;
- - учет требований уполномоченных федеральных органов исполнительной власти, ответственных за обеспечение ИБ, к уровню подготовки специалистов;
- учет особенностей, связанных с условиями реализации образовательного процесса (наличие «закрытых» специальностей и «закрытых» образовательных компонентов; сочетание значительной фундаментальной естественнонаучной и математической подготовки (как общей, так и специальных разделов математики) и базовой общепрофессиональной подготовки с профилизацией в соответствующей сфере деятельности);
- учет особенностей, связанных с междисциплинарным характером профессиональной области данной группы и содержанием каждой специальности в отдельности.

При определении стратегии подготовки кадров, основываясь на анализе запросов потребителей, считаем целесообразным реализовывать представленный системный подход, позволяющий сравнивать и структурировать различные технические, естественнонаучные и гуманитарные специальности и специализации в области ИБ в зависимости от сфер востребованности выпускников. В частности, он предусматривает подготовку: специалистов как узкого, так и широкого технического и естественнонаучного профиля.

В этой связи в основу определения специальностей данной области и их систематизации был положен объектно-деятельностный подход. Всесторонний анализ сфер, видов, объектов, методов и средств профессиональной деятельности позволил выработать номенклатуру специальностей и специализаций ВО в области информационной безопасности.

Кроме этого, был проведен анализ содержания примерных основных образовательных программ (далее – ПООП) по существующим специальностям. Анализ показывает, что количество дисциплин и объем времени на их реализацию по каждой специальности различается: по достижению общепрофессиональных компетенций естественнонаучной ориентации до 10%, по достижению общепрофессиональных компетенций общепрофессиональной ориентации в пределах 30 – 60%. Имеются достаточные различия по содержанию данных дисциплин, а также полностью различными являются профессиональные компетенции, перечень и содержание дисциплин, формирующих их.

Таким образом, специальности в группе «Информационная безопасность» обладают необходимыми отличительными признаками, определяющими как содержательно-образовательную, так и функционально-деятельностную стороны подготовки специалистов различного профиля.

Данная группа обладает необходимыми отличительными признаками, среди которых важнейшими являются:

- явно выделенная предметная область (сфера, виды, объекты, методы и средства профессиональной деятельности), связанная с защитой информации в системах ее обработки, передачи и хранения;
- совокупность ОПК и ПК, индикаторов их достижения, содержание дисциплин (модулей), их формирующих;
- вполне определенная направленность содержания общих естественнонаучных и общепрофессиональных дисциплин, имеющих существенное отличие от смежных УГСНП в области инфокоммуникационных технологий.

Следует отметить, что в настоящее время ФГОС 3+ и 3++ по направлениям подготовки и специальностям в области ИБ являются достаточно мобильными. ФГОС и разработанные на их основе образовательные программы позволяют адекватно отвечать на вызовы и угрозы в информационной сфере, реализовывать запросы работодателей индустрии информационной безопасности и требования заинтересованных государственных органов, а также учитывать направления научно-технологического развития страны.

При разработке ФГОС ВО 3++ были сформированы новые профили и специализации. Обновление по количеству перечня профилей и специализаций составило более 40 процентов, а по содержанию более 60 процентов, что адекватно отвечает запросам практики на ближайшие 10 лет.

В рамках ФГОС 3++ специалитета реализуются около 50 специализаций. Данные специализации конкретно сопряжены с соответствующими профессиональными стандартами, адресно ориентированы на отрасли экономики и сферы профессиональной деятельности, учитывают современные тенденции и перспективные направления развития индустрии информационной безопасности, требования уполномоченных федеральных государственных органов, а также опыт зарубежных партнеров (Приложение 1).

С учетом изложенного можно констатировать, что существующий Перечень специальностей и направлений подготовки высшего образования и разработанные ФГОС, адекватно отвечают требованиям экономики. Заложенный при разработке Перечня научный, методический и организационный потенциал и на ближайшую перспективу позволяет обеспечивать кадрами все заинтересованные государственные органы, организации и бизнес.

Предлагается структуру существующего Перечня специальностей и направлений подготовки по УГСНП «Информационная безопасность» оставить без изменений (Приложение 2). Данные предложения поддерживаются ключевыми объединениями работодателей, уполномоченными государственными органами в области ИБ, решениями рабочих органов Совета Безопасности Российской Федерации.

Формирование новой области образования в сфере информационно-коммуникационных технологий и включение в нее отдельной УГСНП 10.00.00 «Информационная безопасность» поддерживаем.

Вместе с тем, анализ Стратегии научно-технологического развития Российской Федерации на долгосрочный период, ключевых индикаторов и базовых показателей федеральных проектов «Кадры для цифровой экономики» и «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» (объем подготовки ИТ-специалистов довести до 120 тыс.чел.) и иных стратегических документов в сфере цифровой трансформации экономики и общества, а также итоги работы стратегической сессии Министра науки и высшего образования Российской Федерации В.Н. Фалькова и совещания «Кадры будущего» под председательством Заместителя Председателя Правительства Российской Федерации Д.Н. Чернышенко (Иннополис, 6 марта 2021 г.) обуславливают рас-

ширение границ данной области в части предметных научно-образовательных областей и установления автономии укрупненных групп специальностей и направлений.
С учетом изложенного предлагается новую область образования изложить в следующей редакции: «ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОМПЬЮТЕРНЫЕ НАУКИ».

Подходы к разработке макета ФГОС – 4

В связи с принятием Федерального закона от 26 мая 2021 № 144-ФЗ «О внесении изменений в ФЗ «Об образовании в Российской Федерации» ФГОС ВО разрабатываются: по уровням образования; по специальностям и направлениям подготовки; по укрупненным группам специальностей и направлений подготовки (далее – УГСНП); по областям и видам профессиональной деятельности.

Представленные Координационным советом по области образования «Инженерное дело» и Минобрнауки России макеты ФГОС ВО разработаны исключительно на УГСНП. Анализ Перечня специальностей и направлений подготовки высшего образования, утвержденного приказом Минобрнауки России от 1 февраля 2022 года № 89 показывает, что в составе УГСНП могут находится:

- специальности и направления подготовки, которые могут не иметь единого ядра содержания образовательной программы одинакового для всех, и как следствие, единых общепрофессиональных компетенций на УГСНП;
- специальности и направления подготовки, включенные в УГСНП, могут ориентироваться на разные федеральные государственные органы, соответствующие ФГОС ВО разрабатываются в интересах разных федеральных государственных органов и могут не иметь единого ядра;
- специальности, которые могут иметь разные сроки реализации образовательных программ;
- специальности и направления подготовки, которые могут содержать сведения, составляющие государственную тайну (ФГОС ВО открытые и закрытые);
- специальности и направления подготовки, которые относятся к разным стоимостным группам.

С учетом изложенного, необходимо предусмотреть два макета ФГОС-4: макет ФГОС ВО на УГСНП (предлагаемый Минобрнауки России и Координационным советом по области образования «Инженерное дело») и макет ФГОС ВО для отдельных специальностей и направлений подготовки.

В соответствии с частями 1 – 4 статьи 11 Федерального закона № 273 ФГОС обеспечивают единство образовательного пространства и государственные гарантии качества образования, поэтому требования стандартов должны быть едиными для всех образовательных организаций. Считаем, что при разработке новых ФГОС ВО четвертого поколения в области ИБ предлагается сохранить расширенные требования к материально-техническому, учебно-методическому и кадровому обеспечению программ бакалавриата, специалитета и магистратуры, включенные в ФГОС ВО 3++.

И самое главное, предлагается в структуру новых ФГОС ВО четвертого поколения включить требования к индикаторам достижений результатов освоения образовательных программ, заменив слова «индикаторы» на «планируемые результаты достижения компетенций», указав в конкретной редакции показатели данных результатов – «знать», «уметь» и «владеть».

Регламентацию практики изложить в следующей редакции: «Наименования, виды (типы), способы проведения и количество практик устанавливаются Организацией самостоятельно. Для выполнения выпускной квалификационной работы проводится преддипломная практика, которая является обязательной. При реализации программы Организация осуществляет проведение практик в организациях, деятельность которых соответствует направленности (профилю) программы, или в структурных подразделениях Организации, предназначенных для проведения практической подготовки выпускников».

Пункт 6.3.2. (для бакалавриата, специалитета, магистратуры) изложить в следующей редакции: «6.3.2. Организация должна быть обеспечена необходимым комплектом лицензионного и (или) свободно распространяемого программного обеспечения, в том числе отечественного производства (состав определяется в рабочих программах дисциплин (модулей) и подлежит обновлению при необходимости)».

Дополнительно в макет включить пункт для разработчиков в следующей редакции: «Разработчики ФГОС в целях достижения качества подготовки выпускников и с учетом особенностей программы (бакалавриата, специалитета, магистратуры) устанавливают дополнительные, особые требования к материально-техническому и учебно-методическому обеспечению реализации Программы (например: перечень лабораторий и функционального оборудования, аудиторию (защищаемое помещение) для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа и т.д.)».

Дополнительно в макет включить пункт для разработчиков в следующей редакции: «Разработчики ФГОС в целях достижения качества подготовки выпускников и с учетом особенностей программы (бакалавриата, специалитета, магистратуры) устанавливают дополнительные, особые требования к кадровым условиям реализации Программы (например: доля штатных педагогических работников, доля ученых по конкретной научной области и т.д.)».

Приложение 1

Перечень открытых профилей и специализаций УГСНП 10.00.00
Информационная безопасность

Бакалавр	КБ	ИБТКС	ИБАС	ИАСБ
1. «Безопасность компьютерных систем» (по отрасли или в сфере профессиональной деятельности); 2. «Организация и технологии защиты информации» (по отрасли или в сфере профессиональной деятельности); 3. «Техническая защита информации»; 4. «Безопасность автоматизированных систем» (по отрасли или в сфере профессиональной деятельности); 5. «Безопасность телекоммуникационных систем» (по отрасли или в сфере профессиональной деятельности); 6. «Информационно-аналитические системы финансового мониторинга»	1. «Анализ безопасности компьютерных систем»; 2. «Математические методы защиты информации»; 3. «Разработка защищенного программного обеспечения»; 4. «Безопасность компьютерных систем и сетей» (по отрасли или в сфере профессиональной деятельности); 5. «Разработка систем защиты информации компьютерных систем объектов информатизации» (по отрасли или в сфере профессиональной деятельности); 6. «Информационно-аналитическая и техническая экспертиза компьютерных систем»;	6. «Информационная безопасность аэрокосмических ТКС; 7. «Разработка защищенных ТКС»; 8. «Защита информации в радиосвязи и телерадиовещании»; 9. «Управление безопасностью ТКСиС»; 10. «Информационная безопасность мультисервисных телекоммуникационных сетей и систем на транспорте» (по видам); 11. «Системы подвижной цифровой защищенной связи»; 12. «Техническая защита информации информационно-телекоммуникационных систем».	5. «Безопасность открытых информационных систем»; 6. «Безопасность автоматизированных систем в финансово-кредитной сфере»; 7. «Анализ безопасности информационных систем»; 8. «Разработка автоматизированных систем в защищенном исполнении»; 9. «Безопасность автоматизированных систем на транспорте» (по видам); 10. «Безопасность автоматизированных систем управления технологическими процессами» (по отрасли или в сфере профессиональной деятельности); 11. Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности);	2. «Автоматизация информационно-аналитической деятельности»; 3. «Информационная безопасность финансовых и экономических структур»; 4. «Технологии информационно-аналитического мониторинга»; **БИТ в правоохранительной сфере** 4. «Компьютерная экспертиза»; 5. «Организация и технологии обеспечения защиты информации».

Приложение 2

Вариант структуры

Перечня направлений подготовки и специальностей высшего образования

Коды УГСН	**Наименования областей образования, УГСН, направлений подготовки и специальностей**	**Присваиваемые квалификации по уровням высшего образования**
ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОМПЬЮТЕРНЫЕ НАУКИ		
32	Фундаментальная информатика и математическое обеспечение компьютерных наук	
33	Информатика, вычислительная техника и искусственный интеллект	
34	Информационная безопасность	
	Информационная безопасность	Бакалавр информационной безопасности Магистр информационной безопасности
	Компьютерная безопасность	Специалист по защите информации
	Информационная безопасность телекоммуникационных систем	Специалист по защите информации
	Информационная безопасность автоматизированных систем	Специалист по защите информации
	Информационно-аналитические системы безопасности	Специалист по защите информации
	Безопасность информационных технологий в правоохранительной сфере	Специалист по защите информации
	Криптография	Математик, специалист по защите информации
	Противодействие техническим разведкам	Специалист по защите информации

Список литературы

1. Приказ Министерства науки и высшего образования Российской Федерации от 01.02.2022 **№ 89** «Об утверждении перечня специальностей и направлений подготовки высшего образования по программам бакалавриата, программам специалитета, программам магистратуры, программам ординатуры и программам ассистентуры-стажировки» (Зарегистрирован 03.03.2022 № 67610).
2. Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 **№ 273-**ФЗ.

УДК 378.046.4

О РАЗВИТИИ ИНТЕЛЛЕКТУАЛЬНОГО ПОТЕНЦИАЛА ЦИФРОВОЙ ТРАНСФОРМАЦИИ РЕСПУБЛИКИ БЕЛАРУСЬ

И.В. МЯЧИН, А.Н. ЛЕПЕХИН, О.В. БЕЛЯКОВ
Оперативно-аналитический центр при Президенте Республики Беларусь
г.Минск, 220030, Республика Беларусь

Общепризнанным стратегическим направлением развития общества современном мире, охватывающим экономику, социальную сферу и государственное управление, является цифровая трансформация.

Актуальность вопросов, связанных со всеми ее проявлениями, подчеркивается также количеством комплексных и частных научных исследований по вопросам изучения информационного общества, цифровой экономики и всех проявлений ее трансформации, анализ которых показывает, что большинство белорусских авторов (А.Н.Курбацкий, М.Г.Зеков и др.) отмечают огромный рывок, который сделала Республика Беларусь за последнее десятилетие в части преодоления цифрового разрыва от ведущих стран мира, что подтверждается и высокими позициями нашей страны в различных мировых рейтингах (индекс развития информационно-коммуникационных технологий, публикуемый Международным союзом электросвязи, исследования Организации Объединенных Наций в области оценки уровня электронного правительства и др.).

Как справедливо отметил Президент Республики Беларусь в своем обращении с Посланием к белорусскому народу и Национальному собранию еще в 2018 году, «взрывной рост новых технологий является одним из ключевых факторов определения развития современного мира» [1].

Сложно не согласиться и с тем, что современные глобальные экономические и социальные изменения ставят перед Республикой Беларусь новые задачи, среди которых повышение национальной конкурентоспособности, придание большей устойчивости государству в условиях экономических и социальных трансформаций. Эти задачи не могут быть решены без новых технологий и новых знаний, без создания инновационной экономики, важнейшим институтом развития которой является система образования. Обществу нужны образованные, нравственные, предприимчивые и компетентные личности, способные самостоятельно принимать ответственные решения в ситуации выбора, прогнозируя их возможные последствия, умеющие выбирать способы сотрудничества. Они должны отличаться мобильностью, динамизмом, конструктивностью, обладать развитым чувством ответственности за свою судьбу и судьбу страны [2].

Стоит отметить, что главой 7 «Цифровая трансформация» Программы социально-экономического развития Республики Беларусь на 2021 – 2025 годы, утвержденной Указом Президента Республики Беларусь от 28 июля 2021 г. № 292, предусмотрено, что в 2025 году доля специалистов, ответственных за вопросы информатизации в государственных органах и организациях, прошедших обучение в сфере цифрового развития, составит не менее 40 процентов.

К слову, в рамках доклада Главе государства об отельных вопросах развития страны в цифровой сфере еще 14 октября 2019 г. Президентом Республики Беларусь обозначено наличие проблемных вопросов, связанных с отсутствием понимания среди большинства

населения терминологии связанной с цифровизацией, информатизацией и компьютеризацией, а также нехваткой специалистов совершенно другого качества для успешной цифровой трансформации и создания новой экономики [3].

Действительно, цифровая трансформация государства, бизнеса и общества в настоящее время является ключевым условием развития страны и повышения ее конкурентоспособности.

Вместе с тем цифровая трансформация – сложная и многогранная работа на самых разных уровнях государства и отрасли, бизнеса и организации, граждан и работников. Такая работа требует специальных организационных механизмов для ее планирования, координации и анализа.

В данной связи очевидно, что развитие интеллектуального потенциала цифровой трансформации должно стать важнейшей задачей, в решении которой государство выступает основным заказчиком, координатором и исполнителем.

В свою очередь, в настоящее время в обиход вошел новый термин «информационная культура», под которым обычно понимается умение человека решать свои повседневные задачи, относящиеся к его профессиональной, общественной и личной жизни, с использованием компьютерных устройств. Сформированная информационная культура позволяет человеку быстро и без особых проблем адаптироваться к быстро меняющемуся миру и приспосабливаться к цифре.

Во многих случаях этого достаточно. Вместе с тем практика показывает, что хорошей информационной культуры недостаточно для «лиц, принимающих решения». Важно понимать, что цифровая эра предполагает неизбежную трансформацию организационных моделей управления. Подготовка управленцев, способных работать в новых условиях, – задача для государства, к которой нужно подходить со всей серьезностью [4].

Учитывая изложенное, видится, что ключевым условием развития интеллектуального потенциала цифровой трансформации выступает именно подготовка руководителей к управлению своими структурами в имеющихся реалиях повсеместного использования современных информационно-коммуникационных технологий, поскольку указанные выше задачи могут быть решены исключительно лицами, принимающими решения.

Справедливо отметить, что сегодня в Республике Беларусь нет учебного заведения, которое могло бы самостоятельно удовлетворить указанную потребность государства, в связи с чем кооперация усилий регуляторов, представителей академической науки, а также лучших практических специалистов ведущих организаций видится очевидной и необходимой.

В свою очередь, актуальным является имеющийся опыт образовательной деятельности республиканского унитарного предприятия «Национальный центр обмена трафиком» (далее – НЦОТ), которое было учреждено Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – ОАЦ) в соответствии с Указом Президента Республики Беларусь от 30 сентября 2010 г. № 515 «О некоторых мерах по развитию сети передачи данных в Республике Беларусь» в целях демонополизации рынка услуг передачи данных, развития современной инфраструктуры сети передачи данных на основе внедрения новых технологий, а также привлечения в эту сферу прямых иностранных инвестиций.

Учитывая имеющуюся потребность, по инициативе ОАЦ и при активной поддержке Министерства образования Республики Беларусь с 1 апреля 2020 г. отделом образовательных услуг НЦОТ начата образовательная деятельность по повышению квалификации лиц, в обязанности которых входит обеспечение информационной безопасности по вопросам технической и (или) криптографической защиты информации.

Принимая во внимание, что современное информационное общество, в котором интенсивно развиваются и применяются информационно-коммуникационные технологии во всех областях общественной жизни, ждет от правительства простого, комфортного, быстрого и эффективного взаимодействия с гражданами и бизнесом, которое может обеспечить электронное правительство, а также тот факт, что его развитие является составным элементом механизма цифровой трансформации экономики, которому ведущие страны мира уделяют особое внимание, с июня 2021 г. на базе НЦОТ осуществляется повышение квалификации по программе обучения «Электронное правительство».

Актуальность реализации указанной учебной программы подтверждается и тем, что состояние электронного правительства, под которым принято понимать новую форму организации деятельности государства, обеспечивающую за счет широкого применения информационно-коммуникационных технологий качественно иной уровень оперативности и удобства получения населением и бизнесом электронных услуг и административных процедур в электронной форме, и эффективность его работы в большей степени определяет уровень достигнутого на текущий момент результата цифровой трансформации в сфере государственного управления.

Эффективность реализуемых в НЦОТ учебных программ была предопределена в большей степени упоминаемым выше подходом по консолидации усилий регуляторов, лекторов ведущих учреждений высшего образования и лучших практических специалистов.

Стоит также отметить проведение на регулярной основе методичной работы по совершенствованию образовательного процесса, внедрению новых востребованных техник и методик преподавания, что прежде всего обусловлено стремительным устареванием компетенций в сфере информационно-коммуникационных технологий, приобретаемых в настоящее время.

Так, программные продукты крупнейших компаний претерпевают значительные изменения в среднем каждые два-четыре года, что требует регулярного отслеживания за обновлениями программ и отдельных модулей. Технические изменения происходят еще быстрее. Разумеется, основы создания архитектуры информационных систем меняются гораздо медленнее и эти знания устаревают не так быстро, но для эффективной работы по данному направлению в любом случае требуется регулярное обновление имеющихся знаний [5].

Дополнительно стоит отметить значимость объединения усилий и обеспечения эффективного взаимодействия всех государств – участников Содружества Независимых государств. К слову, стратегией сотрудничества государств – участников СНГ в построении и развитии информационного общества на период до 2025 года, утвержденной принятым в г.Минске решением Совета глав правительств Содружества Независимых Государств от 28 октября 2016 г., предусмотрено, что главными движущими силами развития информационного общества становятся технологии получения и практического применения новых знаний, а подготовка квалифицированных кадров отнесена к одной и основных задач, стоящих перед государствами-участниками.

В этой связи в марте 2022 г. в структуре НЦОТ произошло изменение организационно-штатной структуры, вследствие чего упомянутый отдел образовательных услуг трансформирован в Международный центр образования, основная задача которого заключается не только в осуществлении образовательной деятельности по вопросам цифровой трансформации, но и в организации и проведении различных международных, республиканских и региональных мероприятий (форумов и др.) по тематикам, связанным со всеми проявлениями цифровой трансформации.

К слову, уже 18 – 19 мая 2022 г. в г.Минске состоялся II Международный форум #GBC (Государство. Бизнес. Граждане), проведение которого способствует достижению заявленных целей социально-экономического развития, дополнительному освещению значимости вопросов обеспечения информационной безопасности государства и финансовой независимости в санкционных условиях, а также популяризации созданной в стране информационно-коммуникационной инфраструктуры.

В настоящее время усилия представителей Международного центра образования НЦОТ сконцентрированы на разработке и качественном наполнении учебных программ, ведется активное сотрудничество с высшими учебными заведениями Республики Беларусь (в марте – апреле 2022 г. совершено ряд меморандумов о намерениях по сотрудничеству в сфере информационно-коммуникационных технологий), представителями бизнеса и государственных органов-регуляторов.

В этой связи видится уместным масштабировать имеющийся опыт НЦОТ в части трансформации системы повышения квалификации в сфере кибербезопасности на всю страну, в первую очередь путем объедения усилий указанных выше субъектов в целях дачи таргетированных и актуальных знаний конкретным руководителям нашей страны, разработки качественных образовательных программ, дифференцированных не только в зависимости от отрасли, но и уровня руководителя-слушателя, а также реализации передовых форматов обучения для лидеров, способных применить полученные знания на благо своей наших граждан и страны.

Список литературы

1. Послание белорусскому народу и Национальному собранию [Электронный ресурс] // Официальный Интернет-портал Президента Республики Беларусь. – Режим доступа: https://president.gov.by/ru/events/poslanie-k-belorusskomu-narodu-i-natsionalnomu-sobraniju-18594. – Дата доступа: 20.04.2022
2. О Концепции развития системы образования Республики Беларусь до 2030 года [Электронный ресурс] : постановление Совета Министров Респ. Беларусь, 30 нояб. 2021 г., № 683 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2022.
3. Доклад об отдельных вопросах развития страны в цифровой сфере [Электронный ресурс] // Официальный Интернет-портал Президента Республики Беларусь. – Режим доступа: https://president.gov.by/ru/events/soveschanie-po-razvitiju-tsifrovoj-sfery-22208#block-after-media-scroll. – Дата доступа: 20.04.2022.
4. Курбацкий, А. Н. Цифра и власть: первое погружение : 50 вопросов заинтересованного чиновника / А. Н. Курбацкий, М. Г. Зеков. – Минск : Академия управления при Президенте Республики Беларусь, 2021. – 192 с.
5. Лепехин, А. Н. О практике повышения квалификации в сфере информационной безопасности / А. Н. Лепехин, И. В. Мячин // Комплексная защита информации : материалы XXVI науч.-практ. конф., г. Минск, 25-27 мая 2021 г. – Минск: Издатель Владимир Сивчиков, 2021. – С. 165–168.

УДК 004.056.5

ПОДГОТОВКА СПЕЦИАЛИСТОВ ПО КИБЕРБЕЗОПАСНОСТИ В БГУИР

Т.В. БОРБОТЬКО
Белорусский государственный университет информатики и радиоэлектроники,
Минск, 220013, Беларусь

Широкое использование информационных систем в различных сферах деятельности человека позволяет обеспечить соответствующие бизнес-процессы и создать условия для благоприятного развития таких направлений. Вместе с тем, устойчивое развитие различных сфер деятельности требует также совершенствования методов и средств обеспечения кибербезопасности подобного рода систем, то есть создания таких условий их функционирования, при которых информационные системы и содержащаяся в них информация защищены от внешних и внутренних угроз [1].

Доступность информационных систем из глобальной сети Интернет обуславливается необходимостью их использования различными участниками подобного информационного обмена и вместе с тем, создает условия для проведения целенаправленных программных или программно-технических воздействий на их объекты, сети электросвязи, посредством которых такие объекты взаимодействуют, с целью нанесения ущерба их владельцам. Ежегодное усиление этой проблемы [2] в мире обуславливается геополитическим взаимодействием крупных государств таких как США, КНР, Российская Федерация и других. Текущее положение дел обуславливает необходимость совершенствования процесса и направлений подготовки кадров по информационной безопасности в Республике Беларусь.

В Белорусском государственном университете информатики и радиоэлектроники (БГУИР) накоплен значительный опыт подготовки кадров в сфере информационной безопасности. В 2004 году для обеспечения выпуска таких специалистов была создана кафедра защиты информации. В настоящее время подготовка кадров реализуется по специальности 1-98 01 02 «Защита информации в телекоммуникациях» на первой ступени высшего образования с присвоением квалификации «специалист по защите информации, инженер по телекоммуникациям» и специальности 1-98 80 01 «Информационная безопасность» профилизации «Защита информации в информационных системах» второй ступени высшего образования с присвоением степени магистр. Учебный план по первой указанной выше специальности включает рассмотрение ряда вопросов, исходя из запросов заказчиков кадров. Таким образом, в рамках специальных учебных дисциплин рассматриваются: инженерно-техническая защита объектов, защита информации от утечки по техническим калам, обеспечение безопасности информации обрабатываемой в информационных системах, криптографическая защита информации. Углубленное рассмотрение вопросов связанных с обеспечением защиты информации обрабатываемой в информационных системах реализовано в рамках специальности 1-98 80 01 «Информационная безопасность».

Анализируя текущее положение дел в области подготовки специалистов по информационной безопасности в БГУИР, а также потребности кадров по информационной безопасности в Республике Беларусь, целесообразным представляется открытие новой специальности (профилизации) по информационной безопасности в БГУИР – «Кибербезопасность» на базе кафедры защиты информации.

В рамках указанной специальности (профилизации) подготовку специалистов планируется проводить с учетом современных потребностей заказчиков кадров, в рамках которой у обучающегося будут формироваться компетенции по следующим направлениям:

1. Проектирование, создание и эксплуатация защищенных информационных систем;
2. Анализ и фильтрация трафика в информационных сетях;
3. Идентификация, аутентификация и авторизация субъектов доступа в информационных системах;
4. Криптографическая защита информация в информационных системах;
5. Обнаружение и реагирование на инциденты информационной безопасности в информационных системах.

Для обеспечения образовательного процесса требуется соответствующая лабораторная база. С учетом последних событий связанных с доступностью средств защиты информации импортного производства, в качестве технологической платформы обеспечивающей интеграцию средств защиты информации и формирование замкнутого цикла управления информационной безопасностью в БГУИР развернуто программное обеспечение компании R-Vision (Российская Федерация), в частности Incindent Response Platform (IRP) и Threat Intelligence Platform (TIP). Указанные платформы используются на предприятиях Республики Беларусь и их применение в образовательном процессе позволит обеспечить практикоориентированную подготовку специалистов. Реализацию остального перечня компетенций планируется выполнить за счет использования уже существующих на кафедре защиты информации возможностей лабораторной базы. Формируемая таким образом лабораторная база позволит обеспечить в перспективе проведение таже научно-исследовательских работ связанных с созданием, совершенствованием и обеспечением функционирования систем обнаружения, предупреждения и ликвидации последствий компьютерных атак на объекты информатизации.

Список литературы

1. Концепция информационной безопасности Республики Беларусь, утвержденная Постановлением Совета Безопасности Республики Беларусь № 1 от 18 марта 2019 г.
2. Кибербезопасность 2021-2022. Тренды и прогнозы // Positive Technologies [Электронный ресурс]. – 2022. – Режим доступа : https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-2021-2022-trendy-i-prognozy/ – Дата доступа : 11.04.2022.

УДК 004.056

ВЛИЯНИЕ ЧЕЛОВЕЧЕСКОГО КАПИТАЛА НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ В КОНТЕКСТЕ КАЧЕСТВА ОБРАЗОВАНИЯ

С.Н. КАСАНИН[1], А.А. ОХРИМЕНКО[2]
[1]Государственное научное учреждение «Объединенный институт проблем информатики Национальной академии наук Беларуси»,
г. Минск, 220012, г. Минск, Республика Беларусь
[2]Обособленное подразделение «Институт информационных технологий» учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, 220037, Республика Беларусь

Введение

Информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [1].

Последние события, происходящие в мире, показали, что весьма четко обозначилась новая реальность – возможности государства по обеспечению максимального контроля информационных потоков.

Информационная сфера превращается в системообразующий фактор жизни людей, обществ и государств. Усиливается роль и влияние средств массовой информации и глобальных коммуникационных механизмов на экономическую, политическую и социальную ситуацию. Информационные технологии нашли широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями. Происходит эволюция информационного противоборства как новой самостоятельной стратегической формы глобальной конкуренции. Распространяется практика целенаправленного информационного давления, наносящего существенный ущерб национальным интересам [1].

В Республике Беларусь вопрос суверенитета в информационной сфере является одним из наиболее актуальных. Информационная независимость Республики Беларусь получила дополнительную защиту с принятием постановления Совета Безопасности Республики Беларусь от 18 марта 2019 г. №1 «О Концепции информационной безопасности Республики Беларусь» (далее – Концепция). Согласно Концепции, информационный суверенитет – это неотъемлемое и исключительное верховенство права государства самостоятельно определять правила владения, пользования и распоряжения национальными информационными ресурсами, осуществлять независимую внешнюю и внутреннюю государственную информационную политику, формировать национальную информационную инфраструктуру, обеспечивать информационную безопасность [2].

Исходя из определения можно сделать вывод о том, что информационный суверенитет есть ни что иное, как важнейший, основополагающий инструмент обеспечения информационной безопасности.

В связи с вышеизложенным, очевидна необходимость иметь определённой человеческий капитал, другими словами хорошо подготовленных специалистов, обладающих соответствующими компетенциями в области информационной безопасности.

1. Человеческий капитал как индикатор качества образования

Под человеческим капиталом будем понимать «совокупность врожденных способностей и приобретенных знаний, навыков и мотиваций» человека, среду интеллектуального и управленческого труда и обитания, которые обеспечивают качественный и высокопроизводительный труд, способствуют увеличению дохода и улучшению качества жизни (на уровне индивида, корпорации или общества) [3].

Человеческий капитал является одним из наиболее существенных факторов экономического роста и общественного развития стран и наций мира. Национальный человеческий капитал составляет более половины национального богатства каждой из развивающихся стран и свыше 70-80 % – развитых стран мира [4].

Оценки экспертов всех стран мира – от высокоразвитых до развивающихся и бедных – свидетельствуют о том, что отдача от человеческого капитала существенного превышает отдачу от физического капитала. В результате исследования факторов экономического ро-

ста в 192 странах Всемирный банк пришел к выводу, что только 16% роста в странах с переходной экономикой обусловлены физическим капиталом (оборудование, здания и производственная инфраструктура), 20% – природным капиталом, в то время как остальные 64% связаны с человеческим и социальным капиталом [5].

По оценкам Всемирного банка, ещё в 1994 г. 76 % национального богатства США составлял человеческий капитал, физический же (воспроизводимый) капитал представлял 19 % богатства США, а на природный фактор приходились остальные 5 %. В Западной Европе соответственно – 74, 23, 3 %. Благосостояние России держится наполовину (50 %) на человеческом капитале, 10 % дает воспроизводимый капитал и 40 % обеспечивает природа [6].

Одним из базовых составляющими человеческого капитала считаются качество образования. Показатели системы образования являются также основанием для количественной оценки степени эффективности использования человеческого капитала в экономике. Согласно данным этих расчётов, в наиболее развитых странах мира до 40 % валового национального продукта получается в результате развития эффективной системы образования. По данным американских экспертов, каждый доллар затрат в системе образования дает 3-6 долларов прибыли. В современной экономике знаний роль образования существенно возросла. «Развитие человеческого капитала через развитие системы образования» – такова формула успеха в современной конкурентной борьбе за высокое качество жизни и устойчивое развитие общества знания.

В 14-м издании Глобального инновационного индекса (ГИИ) (выпущено 20 сентября 2021 г.) Республика Беларусь заняла 62-е место, улучшив свой рейтинг на 2 позиций по сравнению с 2020 годом (64-е место) или на 24 позиции в сравнении с 2018 годом (86-е место). С учетом показателей Индекса, Беларусь производит больше инновационной продукции по сравнению с уровнем затрат на инновации. Наиболее высокие позиции наша страна занимает по укрупненным индикаторам «Знания и технологический выход» (37-е место), «Человеческий капитал и исследования» (38-е место) и «Инфраструктура инноваций» (59-е место). Улучшение рейтинга Беларуси отражает итоги проводимой Правительством Беларуси работы по развитию образовательной среды для инноваций, доступа к ИКТ-технологиям, разработки инновационных решений в сфере информационных технологий и экспорта ИТ-услуг.

В рейтинге по Индексу человеческого развития (Human Development Indicators) Беларусь входит в группу 30 наиболее развитых стран мира и имеет лучший результат среди стран СНГ (14 позиция вместе с Японией и Латвией).

В рейтинге по индексу уровня образования в странах мира (Education Index) – комбинированному показателю Программы развития ООН (ПРООН) Беларусь находится на 21 месте.

2. Система образования Республики Беларусь для формирования человеческого капитала

По состоянию на начало 2021-2022 учебного года в Республике Беларусь функционирует 50 учреждение высшего образования из них (далее – УВО), не включая Институт подготовки научных кадров Национальной академии наук Республики Беларусь, из них 8 учреждений частной формы собственности.

Из 42 государственных УВО 31 являются университетами, 9 – академиями, 2 – институтами. Профессорско-преподавательский состав УВО республики включает 19,1

тыс. преподавателей, из них: 1,1 тыс. чел. – доктора наук, 7,7 тыс. чел. – кандидаты наук. Ученое звание профессора имеют 0,9 тысячи человек, доцента – 6,7 тыс. чел. [7].

В 2020-2021 учебном году показатель количества обучающихся (студентов, курсантов, магистрантов, слушателей) в учреждениях высшего образования среди стран СНГ в расчете на 10 000 человек населения наибольший в Кыргызстане – 328 чел. В тройку лидеров по данному показателю также вошли Казахстан – 305 чел. и ***Беларусь – 280 чел. (273– 2021-2022)***.

На условиях оплаты обучаются 85,6 тыс. студентов УВО системы Министерства образования (что составляет 53,45% от общей численности). За счет средств предприятий и организаций – 0,5 тыс. чел. и за счет собственных средств – 85,1 тыс. чел., что на 3,73% меньше, чем в прошлом году. Всего в государственных УВО республики на условиях оплаты обучается 118,4 тыс. чел., что составляет 51,8% от общего количества студентов. В сравнении с прошлым годом это на 4,41% больше.

С 2019 года после завершения первой ступени высшего образования или получения среднего специального образования отсрочки от срочной службы с целью получения образования на более высокой ступени (в магистратуре и аспирантуре – после бакалавриата; в вузе – после колледжа) больше не предоставляются.

Количество обучаемых в УВО по годам в Республике Беларусь представлены в таблице 1.

Таблица 1. Количество обучаемых

Показатель	Учебный год					
	2016/ 2017	2017/ 2018	2018/ 2019	2019/ 2020	2020/ 2021	2021/ 2022
Число УВО	51	51	51	51	50	50
Численность студентов, тыс. чел.	313,2	284,3	268,1	260,9	254,4	243
Численность магистрантов, тыс. чел.	11,8	14,9	14,7	11,9	9,0	12,3

По состоянию на начало 2021-2022 учебного года в учреждениях общего среднего образования обучаются 1075,98 тыс. чел. Для сравнения: самое большое количество обучаемых было в 1997-1998 учебном году 1602,1 тыс. чел., самое небольшое 2013-2014 учебном году 931,3 тыс. чел.

Количество учащихся учреждений образования, реализующих образовательные программы среднего специального образования на 10 тыс. чел. населения по состоянию на начало 2021-2022 учебного года в республике составляет 115 чел. Этот показатель с 2009-2010 по 2010-2011 учебный годы постепенно увеличивался, однако начиная с 2011-2012 учебного года, начал снижаться и к 2021-2022 учебному году уменьшился в 1,5 раза.

Количество учащихся учреждений образования, реализующих программы профессионально-технического образования, на 10 тыс. чел. населения по состоянию на начало 2021-2022 учебного года в республике составляет 64 человека. В период с 2012-2013 по 2021-2022 учебные годы, просматривается тенденция устойчивого снижения показателя количества учащихся учреждений образования, реализующих программы профессионально-технического образования, на 10 тыс. чел. Населения. За данный временной промежуток этот показатель уменьшился по республике в 1,3 раза.

Анализ количества обучаемых по странам показывает, что в Республике Беларусь соотношение студентов к общей численности населения одно из самых высоких в Европе и в

мире, кроме того характерен высокий по мировым меркам уровень образования для населения.

По данным 2020 года высшее образование имеют порядка 18 % граждан, 26 % – среднее специальное. По индексу уровня образования населения страна в 2020 году была на 32-ом месте в мире среди 189 стран.

В таблице 2-5 приведены показатели по заработной плате, расходы на образование и соотношение бюджетов по странам [7-9].

Таблица 2. Анализ номинальной начисленной заработной среднемесячной платы работников образования, расходов консолидированного бюджета на образование, инвестиций в основной капитал, направленные на развитие образования

Показатель	Год				
	2016	2017	2018	2019	2020
Номинальная начисленная заработная среднемесячная плата работников образования:					
рублей	551,6	567,5	665,0	774,3	871,7
в % к средне-республиканскому уровню	71,3	69,0	68,5	70,8	69,5
Педагогических работников	585,2	632,4	745,3	900,2	992,2
Профессорско-преподавательского состава	869,1	987,6	1162,5	1357,7	1536,5
Расходы консолидированного бюджета на образование					
млн. руб.	4697	5071	5907	6709	7280
в % к общим расходам консолидированного бюджета	17,2	17,7	17,9	18,6	17,3
Инвестиции в основной капитал, направленные на развитие образования:					
млн. руб.	187,2	249,5	360,9	474,1	537,8
в % к общему объёму инвестиций в основной капитал	1,0	1,2	1,4	1,6	1,8

Таблица 3. Государственные расходы на образование по странам (в процентах к ВВП)

Страна	Год								
	2012	2013	2014	2015	2016	2017	2018	2019	2020
Страны СНГ									
Узбекистан	7,3	7,3	7,3	7,1	6,9	6,4	6,3	6,3	6,3
Кыргыстан	7,0	6,1	5,6	5,9	6,4	6,1	6,0	5,8	6,1
Молдова	8,4	7,0	7,0	6,9	6,3	6,4	6,0	5,8	6,1
Украина	7,0	6,9	6,3	5,7	5,4	6,0	5,9	6,0	6,0
Таджикистан	4,3	5,0	5,1	5,1	5,8	5,9	5,6	5,6	5,4
Беларусь	5,0	5,0	4,8	4,8	4,9	4,8	4,9	4,8	4,7
Казахстан	3,8	3,4	3,4	3,3	3,6	3,5	3,3	3,4	4,5
Россия	3,8	4,1	3,8	3,7	3,6	3,5	3,5	3,7	4,0
Азербайджан	2,7	2,5	2,6	3,0	2,9	2,5	2,5	2,72	3,8
Армения	2,4	2,3	2,4	2,4	2,4	2,2	2,0	2,0	2,3

Страна	Год								
	2012	2013	2014	2015	2016	2017	2018	2019	2020
Страны Евросоюза									
Эстония	4,7	4,8	5,4	5,1	5,2	5,7	6,2		
Латвия	6,6	7,0	5,3	5,3	4,7	5,8	5,8		
Нидерланды	5,5	5,6	5,5	5,4	5,5	5,1	5,1		
Франция	5,5	5,5	5,5	5,5	5,4	5,4	5,1		
Австрия	5,5	5,5	5,4	5,5	5,5	4,8	4,8		
Германия	4,9	4,9	4,9	4,8	4,8	4,1	4,2		
Испания	4,4	4,3	4,3	4,3	4,2	4,0	4,0		
Другие страны									
Австралия	4,9	5,2	5,2	5,3	5,3	5,3	5,4		
Япония	3,7	3,7	3,6	3,5	3,4	3,1	3,1		

Таблица 4. Доходы, расходы государственного бюджета (не консолидированного) стран мира

№ п.п.	Страна	Доходы, млн. $	Расходы млн. $	Год
1	США	5 923 829	9 818 534	2020
2	Китай	3 622 313	5 388 814	2020
3	Германия	1 729 224	2 038 247	2020
15	Россия	337 333	330 667	2021
58	Украина	52 796	59 464	2021
68	***Беларусь***	***23 300***	***27 350***	***2021***

Таблица 5. Список стран по валовому внутреннему продукту (с учётом паритета покупательной способности) на душу населения в долларах США

№	Страна	Данные ВБ[8]	Данные МВФ[9]	№	Страна	Данные ВБ	Данные МВФ
		2020	2021			2020	2021
1	Люксембург	117500	131875	52	Латвия	31464	34707
2	Сингапур	98520	116487	59	Россия	29812	30850
3	Ирландия	93181	112463	61	Казахстан	26754	28387
11	США	63593	69231	***75***	***Белоруссия***	***20239***	***21690***
16	Нидерланды	59268	62841	80	Китай	17211	19260
18	Исландия	53622	59792	84	Туркмения	15200	17721
19	Австрия	55684	59692	96	Азербайд-жан	14480	15882
22	Германия	54792	58378	97	Молдавия	13000	15406
24	Австралия	53330	56403	99	Армения	13312	14661
28	Франция	46983	51364	101	Украина	13055	14325

№	Страна	Данные ВБ[8]	Данные МВФ[9]	№	Страна	Данные ВБ	Данные МВФ
		2020	2021			2020	2021
34	Италия	41829	46161	130	Узбекистан	7734	8585
38	Япония	42390	44739	152	Киргизия	4965	5298
45	Польша	34240	37786	156	Таджикистан	3858	4329

Наблюдается тенденция к снижению количества обучаемых по направление образования 98 «Информационная безопасность». Сравнительный анализ приема 2021 и 2022 годов представлен в таблице 6.

Таблица 6. Сравнительный анализ приема

Ступени высшего образования	План приема, чел.			
	2021		2022	
	бюджет	платное	бюджет	платное
Первая ступень высшего образования	211	81	185	78
Вторая ступень высшего образования	20	12	18	2

В 2022 году Витебский государственном университете имени П.М. Машерова, не планируется прием по специальности 1-98 01 01-02 Компьютерная безопасность (радиофизические методы и программнотехнические средства). В 2021 году план приема предусматривал 21 чел.

Факультет инфокоммуникаций Белорусского государственного университета информатики и радиоэлектроники в 2022 году не планирует набор в очную форму получения образования в магистратуру по специальности 1-98 80 01 Информационная безопасность и сократил план приема до 8 чел. с 20 чел. в 2021 году (2020 – 30 чел.).

С целью повышения квалификации Постановлением Министерства образования Республики Беларусь от 16 января 2020 № 2 «О предоставлении права реализации образовательной программы повышения квалификации руководящих работников и специалистов» республиканскому унитарному предприятию «Национальный центр обмена трафиком» предоставлено право реализации образовательной программы повышения квалификации руководящих работников и специалистов.

Программа обучения ориентирована на повышение квалификации работников организаций и предприятий всех форм собственности, в обязанности которых входит обеспечение информационной безопасности, в частности решение вопросов технической и (или) криптографической защиты информации.

Программы курсов согласованы с государственным регулятором в сфере технической и криптографической защиты информации – Оперативно-аналитическим центром при Президенте Республики Беларусь.

Обучение направлено на совершенствование компетенций, необходимых для осуществления деятельности в сфере информационной безопасности и (или) повышение профессионального уровня руководителей и специалистов, в том числе в области технической и (или) криптографической защиты информации.

Заключение

Одним из условий поддержания информационной безопасности является качество человеческого капитала. Однако существующие провалы, препятствующие подготовке конкурентоспособного человеческого капитала в системе образования становиться потенциальной угрозой информационной безопасности страны.

Система образования Республики Беларусь имеет ряд преимуществ (доступность, поддержка талантливой молодежи, социальная справедливость и т.п.), однако сочетание высоких показателей по запасам человеческого капитала с низкими показателями уровня ВВП на душу населения свидетельствует, прежде всего, о неэффективности инвестиций в человеческий капитал, а также о наличии проблем в его формировании, развитии и использовании.

Насколько способна в настоящее время система образования производить конкурентоспособный человеческий капитал, своевременно реагировать на скорость происходящих изменений, адаптироваться к их новому содержанию и, следовательно, обеспечивать необходимый уровень информационной безопасности. Постановка проблемы в таком ракурсе требует выявления и описания существующих провалов, препятствующих подготовке конкурентоспособного человеческого капитала в области информационной безопасности. Проблемы заключаются в следующем:

- проблема 1 – увеличивается спрос на *«обладание дипломом о высшем образовании»,* УВО увеличивают количество платных мест приема;
- проблема 1 порождает проблему 2 – УВО увеличивают педагогическую нагрузку, что ведет к увеличению дефицита времени на занятие научно-исследовательской работой профессорско-преподавательского состава, при этом заработная плата растет незначительно или остается прежней;
- проблема 2 порождает проблему 3 – падает качество обучения и результативности научной деятельности;
- проблема 3 порождает проблему 4 – нежелание бизнеса финансировать УВО по причине недостаточных профессиональных компетенций выпускников;
- проблема 5 – недофинансирование со стороны государства (*принцип остаточного финансирования и иллюзия, вызванная высоким спросом, что все издержки можно переложить на потребителя*);
- проблема 6 – автоматизированный процесс зачисления на специальности (*не человек выбирает специальность, а специальность выбирает человека*).

Список литературы

1. Указ Президента Республики Беларусь 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь».
2. Постановления Совета Безопасности Республики Беларусь от 18 марта 2019 г. №1 «О Концепции информационной безопасности Республики Беларусь».
3. Becker, Gary S. Human Capital. — N.Y.: Columbia University Press, 1964.
4. Корчагин Ю.А. Широкое понятие человеческого капитала. – Воронеж. : ЦИРЭ, 2009.
5. Амбросов Ю.А. Инвестиции в человеческий капитал как показатель качества экономического роста. / Ю.А. Амбросов // Актуальные вопросы экономических наук. 2012. № 27. Новосибирск, 2012. С. 100-105.
6. Ишина И.В. Финансово-экономическая база образования: состояние, проблемы, перспективы. – М. : НИИВО, 2001. С. 34

7. Система образования Республики Беларусь в цифрах/ Соломонова В.В., Шнитко А.В., и др. – Минск: Учреждение «Главный информационно-аналитический центр Министерства образования Республики Беларусь», 2022. – 62 с
8. GDP based on purchasing-power-parity (PPP) per capita . Дата обращения: 24 апреля 2022.
9. GDP based on purchasing-power-parity (PPP) per capita Дата обращения: 24 апреля 2022.
10. Кристеневич С.А. Сохранения национального человеческого капитала как фактор экономической безопасности / С.А. Кристеневич // Белорусский экономический журнал – 2017 №4. С. 23-26.

УДК 004.056

О НОВЫХ ПРОФЕССИЯХ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е.Б. БЕЛОВ, В.П. ЛОСЬ, П.Ю. ПУШКИН
МИРЭА - Российский технологический университет,
г. Москва, *119454,* Российская Федерация

В настоящее время в Российской Федерации действуют пять профессиональных стандартов в области информационной безопасности (табл. 1).

Таблица 1.

Наименование стандарта	Дата утверждения
Специалист по защите информации в автоматизированных системах	15.09.2016
Специалист по технической защите информации	01.11.2016
Специалист по безопасности компьютерных систем и сетей	01.11.2016
Специалист по защите информации в телекоммуникационных системах и сетях	03.11.2016
Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности	09.11.2016

В 2021-2022 гг. эти стандарты прошли процедуру актуализации. В настоящее время разрабатываются еще два профессиональных стандарта:

- Специалист по обеспечению безопасности значимых объектов критической информационной инфраструктуры;
- Специалист по криптографической защите информации.

В 2021 году Сбер совместно с Высшей школой экономики опубликовал Атлас профессий будущего [1]. В разделе «Кибербезопасность» в Атласе были указаны следующие профессии:

- Специалист по кибербезопасности облачных сред;
- Специалист по противодействию кибермошенничеству;
- Эксперт по защите персональных данных;
- Специалист по анализу угроз;
- Исследователь уязвимостей.

Рассмотрев эти предложения на Совете по профессиональным квалификациям в области информационных технологий (СПК-ИТ), Совет принял решение об учете этих предложений в следующих форматах (табл. 2): по двум предложениям планируется разработать новые профессиональные стандарты, по остальным позициям учесть эти предложения путем корректировки существующих профессиональных стандартов.

Особую актуальность в настоящее время имеет проблема защиты персональных данных.

Современный этап развития цифрового общества характеризуется вовлечением все большего количества граждан в процессы информационного взаимодействия. Как следствие, и с учетом новых вызовов обществу, связанных, в том числе, с пандемией, количество новых пользователей различных Интернет-приложений резко возросло. Только в I квартале 2020 года спрос на товары российских интернет-магазинов увеличился на 500%. При этом ведущие маркетплейсы зафиксировали более чем двухкратный рост числа новых пользователей.

Таблица 2.

Предложения ВШЭ	Позиция СПК-ИТ	
Специалист по кибербезопасности облачных сред	Актуализация существующих ПС	Учет в ОТФ, ТФ и ТД
Специалист по противодействию кибермошенничеству	Новый ПС	Специалист по противодействию кибермошенничеству
Эксперт по защите персональных данных	Новый ПС	Специалист по защите персональных данных
Специалист по анализу угроз	Актуализация существующих ПС	Учет в ОТФ, ТФ и ТД
Исследователь уязвимостей	Актуализация существующих ПС	Учет в ОТФ, ТФ и ТД

Сбор и обработка персональных данных граждан всегда связаны с угрозами безопасности такой информации. Утечки персональных данных происходят периодически и не зависят от материально-технического уровня оператора. За последнее время ряд крупных компаний, обрабатывающих персональные данные, заявили об успешных атаках на свои базы данных. Результаты государственного контроля операторов за 2020 год, организованного Роскомнадзором, показали, что 60% проверок завершаются выдачей предписаний об устранении нарушений законодательства в области персональных данных.

Обязанность обеспечить безопасность персональных данных российским законодательством возложена на операторов, обрабатывающих такую информацию. Требования по защите персональных данных установлены Конституцией Российской Федерации, отдельным Федеральным законом, постановлениями Правительства Российской Федерации, указом Президента Российской Федерации, а также иными подзаконными актами, приказами и методическими документами уполномоченных федеральных органов исполнительной власти. Нормативными актами определена обязанность операторов назначить лиц, ответственных за организацию обработки персональных данных и создать структурные подразделения, ответственные за обеспечение безопасности персональных данных в информационных системах. Очевидно, что каждая организация, а также отдельные индивидуальные предприниматели и самозанятые обрабатывают персональные данные. В официальном реестре на февраль 2022 года содержатся записи о 435918 операторов персональных данных. В большинстве случаев персональные данные – единственная категория информации ограниченного доступа, требующая защиты в организации и, следовательно, специалистов по их защите.

Обработка персональных данных имеет специфические особенности, такие как обезличивание и деобезличивание данных, требования к локализации баз персональных данных и трансграничной передаче, использованию и хранению биометрической информации, учет международных требований при обработке персональных данных иностранных граждан, наличие прав и обязанностей субъекта персональных данных. Специалист по защите персональных данных, в большинстве случаев, должен обеспечить все процессы обработки и защиты таких данных: начиная с обследования организации документооборота оператора и подачи уведомления об обработке персональных данных до реализации технических мер и оценки эффективности их защиты. При этом, в отличии от защиты иной информации ограниченного доступа, специалист по защите персональных данных должен обеспечить выполнение требований и, в ряде случаев, прохождение контроля сразу трех уполномоченных федеральных органов исполнительной власти (РКН, ФСБ России, ФСТЭК России), а также выполнение иных ведомственных и отраслевых стандартов и требований.

Поэтому введение нового профессионального стандарта по данному виду профессиональной деятельности, охватывающего сферы организации и технологий защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных, представляется весьма своевременной и важной государственной задачей.

В проекте профессионального стандарта предлагается использовать пять основных трудовых функций:

- проведение работ по обеспечению безопасности персональных данных в организациях (ОТФ1 – 5 уровень квалификации);
- обеспечение комплексной безопасности информационных систем персональных данных в соответствии с их уровнем защищенности (ОТФ2 – 6 уровень квалификации);
- защита персональных данных в государственных информационных системах (ОТФ3 – 6 уровень квалификации);
- разработка систем защиты персональных данных (ОТФ4 – 7 уровень квалификации);
- формирование требований к системе защиты персональных данных (ОТФ5 – 8 уровень квалификации).

Профессиональный стандарт «Специалист по защите персональных данных» предлагается разработать следующими организациями: АНО ДПО ЦПК «АИС»; АЗИ, ФГБОУ ВО «РТУ МИРЭА», Академией ФСБ России, Федеральным учебно-методическим объединением по образованию в области информационной безопасности (ФУМО ВО ИБ) в целях реализации Указов Президента Российской Федерации от 7 мая 2012 года №596 «О долгосрочной государственной экономической политике», от 15 января 2013 года №597 «О мероприятиях по реализации государственной социальной политики», Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 31 марта 2014 года №487-р и протокольного решения Минтруда России от 8 февраля 2015 года №14-3/10/П-576 по итогам совещания по вопросу «О разработке профессиональных стандартов специалистов по группе занятий (профессий) «Специалисты в области информационной безопасности».

Список литературы

1. Атлас профессий будущего: [Электронный ресурс]. URL: https://www.sberbank.ru/atlas#/. (дата обращения 01.06.2022).

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: КАДРЫ И ОБРАЗОВАНИЕ РЕШАЮТ ВСЕ

А.Г.СТОППЕ

Постоянный Комитет Союзного государства
г. Москва, 125340, Российская Федерация

В современном мире одним из важнейших товаров все в большей степени становятся человеческий капитал и интеллектуальная собственность. В Союзном государстве за годы его существования удалось сформировать единое образовательное и единое научно-технологическое пространство, а также сохранить достаточно высокий потенциал человеческого капитала и связанную с ним способность создавать интеллектуальную собственность.

Сегодня, когда Россия и Беларусь подвергаются беспрецедентному санкционному давлению, когда остро стоит проблема импортозамещения, вопросы инновационного развития, обеспечения интеллектуальной и информационной безопасности приобретают приоритетное значение.

Кроме того, в стремительно меняющемся мире, в условиях гибридной войны, нарушения основополагающих принципов частной собственности и экономического суверенитета, именно динамизм и оперативная адаптация к начавшейся пятой, а по некоторым оценкам, уже шестой технологической революции являются гарантиями устойчивого развития государства и благосостояния его граждан.

Говорят: молодежь – наше будущее. Прежде всего – она наше настоящее. Особенно – современная, родившаяся в XXI веке, выросшая в условиях цифровизации и глобальной информатизации. Поэтому кому, как не ей, умеющей быстро приспосабливаться к меняющейся обстановке, стать основной силой развития страны.

Молодому человеку нужно поле для проявления себя, своей индивидуальности. Он хочет быть успешным, уважаемым в обществе человеком. Как ему это доказать? Как социализироваться? Где молодой человек сегодня может проявить себя как личность?

Политика, наука, бизнес – здесь у молодежи есть колоссальные возможности, особенно на научном и экономическом поле деятельности. Перед каждым молодым человеком стоит тема выбора направления деятельности, но правильный выбор можно сделать только тогда, когда хорошо представляешь себе, к чему у тебя талант, на каком направлении ты можешь стать успешным. А без качественного образования в связке не только со знаниями, но и умением анализировать, думать, чем всегда славилась советская система образования – это как бег на одной ноге. И какая бы работа не была выбрана, везде присутствует тема защиты информации – и к этому надо быть готовым.

В рамках Союзного государства белорус в России, а россиянин в Беларуси чувствует себя как в своей стране, как это было многие века. Белорусы и россияне на территории двух стран пользуются равными социальными гарантиями, свободой передвижения, трудоустройства, доступом к медицинским и образовательным услугам. Не нужно оформлять разрешение на работу. Взаимно признается трудовой стаж для получения пенсии по выслуге лет. Многие пользуются достигнутым как само собой разумеющимся, даже не отдавая себе отчета в том, что это не «манна небесная», а результат союзного строительства.

Что касается молодежи, то сформированные в Беларуси и России общее образовательное, научно-технологическое, информационное, правовое пространство, объединенная транспортная система создают для молодежи синергетический эффект для приложения своих сил и самореализации.

Одним из наиболее заметных направлений союзного строительства является реализация программ Союзного государства. Большинство из них направлено на создание инновационного продукта и прорывных технологий в сфере освоения космоса, электронной промышленности, информационных систем, новых видов материалов и высокотехнологичных приборов. При этом совместные российско-белорусские проекты – это, прежде всего, результат консолидации научных и технических сил двух стран, создания новых интеллектуальных ресурсов и компетенций. В этих коллективах, конечно, присутствует молодежь. Вместе с тем есть замысел о выделении специальных грантов для молодежных научных проектов, например, совместно с национальными академиями наук.

Есть идея запуска единого информационного молодежного интернет-портала, который мог бы стать своеобразной «витриной» молодежных проектов, позволил бы оперативно информировать молодежь о мерах государственной поддержки.

Важная тема – академическая мобильность. Здесь большую роль играет система выбора Альма-матер, потому что чем шире выбор, тем большая вероятность того, что молодой человек выберет именно тот вуз, который ему подходит, в комплексе: знания, комфорт проживания, материальные возможности, культурная среда.

В Союзном государстве в последние годы существенно активизировалась молодежная политика, причем в самых разных сферах и, в первую очередь, в области поддержки творческой молодёжи в науке, высоких технологиях, экономике, литературе, искусстве, в области информационных ресурсов и их защиты.

Есть проекты для гуманитариев: проводится российско-белорусский молодежный конкурс «Союзная лига дебатов», Конкурс молодых международников им. А.А.Громыко, различные творческие и образовательные проекты.

В Брянском государственном университете, например, в прошлом году был организован летний лагерь для студентов из Беларуси. Студенты из Гомельского и Могилевского госуниверситетов в течение двух недель прошли обучение по профессиональным программам.

Говоря об инновациях и молодежном бизнесе, мы подразумеваем прогресс, а говоря о прогрессе, мы подразумеваем не только развитие экономики, но и гуманитарного и информационного сотрудничества, высококачественное образование, в ходе получения которого, кстати, могут завязываться и связи между студентами из разных стран, которые «выстрелят» в будущее в виде интеграционных инновационных бизнес-проектов.

Еще одна важная тема - уровни инновационного процесса. Их количество и содержание является в определенной степени показателем экономического развития страны. Речь идет о государственном, региональном, муниципальном, фирменном и индивидуальном уровнях.

В этой связи необходимо всячески развивать не только сложившиеся центры, но и региональные. Страна сильна своими регионами, а регионы - своими достижениями, конкурентоспособной продукцией, основу которой формируют инновации. Кроме того, это новые рабочие места, заинтересованность населения жить на своей малой родине. Поэтому и в региональных вузах образование в области информационной безопасности должно стать таким же важным направлением, как в 90-е годы прошлого века – информатизация.

На предыдущих форумах автор неоднократно поднимал вопрос о Национальной системе индексов научного цитирования. Эта система, нацеленная на приоритетность цитирования в зарубежных изданиях, имеющих более высокий индекс цитирования по сравнению с российскими, применялась как критерий при оценке деятельности академических институтов, вузов, прохождении конкурсов, при переизбрании или замещении вакантных должностей, наносила ущерб интеллектуальной безопасности страны.

Российские ученые были поставлены перед необходимостью публикации своих работ в первую очередь в зарубежных изданиях, а затем уж в российских. Естественно, что тем самым наносился косвенный ущерб защите интеллектуальной собственности, так как любой достаточно высококвалифицированный специалист сможет разобраться из публикации в чем состоит «изюминка» инновации. Таким образом, «Web of Science» и «Scopus» стали мощнейшим геополитическим оружием, направленным на ограбление интеллектуальной собственности российской науки, фиксирование ее позиции в разделе «догоняющей». Все это не могло не сказываться на подготовке молодых специалистов в области информационной безопасности, как минимум, в психологическом плане.

Еще одним легальным путем утечки информации, причем вместе с ее носителями, была Болонская система. Если советская система образования была направлена на то, чтобы подготовить высококлассного специалиста для своей страны, то болонская система, прикрываясь «одеждами» академической мобильности в определенной степени провоцировала утечку талантливой молодежи за границу.

Основными причинами перехода на Болонскую систему было стремление к признанию российских дипломов в Европе и увеличение академической мобильности. Вместе с тем западные университеты до настоящего времени «автоматически» не признают дипломы российских вузов, не удалось создать с ними систему развитой академической мобильности. Большая часть вузов страны работала по двусторонним соглашениям, предусматривающим обучение студентов частично в России, частично за рубежом. Речь идет о двойных дипломах, но это не имеет никакого отношения к Болонскому процессу.

«Бастионы» *«Web of Science»* и *«Scopus»* пали, очередь за Болонской системой (на момент подготовки доклада еще не было известного заявления Министра науки и высшего образования России В.Фалькова о том, что ведомство намерено отказаться от Болонской системы и разработать свою собственную систему высшего образования).

Ключевой вопрос в том, что Болонская система имеет не только минусы, но и определённые ценности и достижения. Надо четко проводить границу между присутствующими в ней задачами академической мобильности, в том числе, обучения за рубежом, и самим содержанием образования. Поэтому, когда мы говорим о новой системе образования, мы должны иметь в виду в первую очередь эволюцию системы образования, которая вберет в себя как достоинства и опыт советской системы образования, так и Болонской.

Перед нами стоит очень сложная задача – соединить обе практики и создать современную, самую лучшую в мире, российскую систему образования, какой она и была практически со времен Ломоносова и Петра Великого.

Беларусь в большей степени, чем Россия, сохранила советскую систему образования, и на основе сформированного в Союзном государстве общего образовательного пространства, использования совместного опыта можно добиться синергетического эффекта в повышении качества подготовки специалистов с высшим образованием, в том числе в области информационной безопасности

Важно использовать уникальный опыт вузов Москвы, Санкт-Петербурга и Минска, Гомеля и Нижнего Новгорода, Гродно и Пскова, Могилева и Казани, сложившиеся прочные межвузовские связи в формировании отвечающей современным требованиям системы образования, вобравшей в себя все лучшие стороны советской и Болонской систем образования.

Необходимо в полном объеме использовать опыт Учебно-методических объединений во главе с ведущими вузами Беларуси и России, причем рассмотреть возможность создания УМО Союзного государства, что позволит унифицировать программы подготовки и быструю адаптацию выпускников, не зависимо от места работы.

В России более 100 вузов, а в Беларуси более 20 различной ведомственной принадлежности осуществляют подготовку специалистов, бакалавров и магистров в области ИБ. Очевидно, что грядущие изменения в системе образования потребуют разработки новых профессиональных стандартов, содержащих все необходимые трудовые функции, расширение номенклатуры образовательных специальностей по защите информации. Эта подготовка должна осуществляться комплексно, охватывая проблемы информационной безопасности не только в научно-технической, но и гуманитарной сферах.

Нельзя забывать и о том, что задача повышения качества подготовки специалистов в области ИБ не может быть решена без совершенствования процесса обучения в вузе, организации педагогического процесса в условиях формирования профессиональной компетентности, повышения квалификационного уровня и профессорско-преподавательского состава. В первую очередь это касается оперативного реагирования на динамичные изменения профессиональной среды, синхронизацию с ее потребностями. Это потребует активного взаимодействия с работодателями, как при разработке содержательной части образовательных программ, так и при выполнении совместных проектов, предоставление производственной базы для организации практик студентов.

К сожалению, не всегда решаются проблемы с обеспечением образовательного процесса высококвалифицированными кадрами и, как следствие, программы обучения по направле-

ниям ИБ имеют тенденцию к отставанию от стремительно меняющейся ситуации в области защиты информации.

Решением большинства этих проблем может стать формирование комфортной для обучаемых и обучающих среды на основе использования положительных сторон Болонской и советской систем образования и российско-белорусского опыта специалитета.

Нельзя также не учитывать тот факт, что крупные IT-компании реализуют совместно с вузами различные программы или открывают свои кафедры в вузах, или филиалы вузовских кафедр у себя. Кроме того, стремительно развивается дополнительное образование, организуются массовые онлайн-курсы. Большинство экспертов считают, что сегодня более половины крупных компаний используют свои возможности для повышения квалификации и доучивания специалистов в области ИБ.

В итоге можно сделать вывод, что система подготовки кадров в области информационной безопасности должна быть самой динамичной, отвечающей современным вызовам угрозам, особенно в условиях информационной войны, которая ведется США и их сателлитами против России и Беларуси. Постоянные изменения, которые претерпевает информационная сфера, диктуют необходимость особого внимания к ней государства, оперативного обновления программ образования и совершенствования системы подготовки специалистов в этой области. Грядущие изменения в системе высшего образования должны проводиться профессионалами, повысить ее эффективность и востребованность, а не стать очередной «перестройкой».

УДК *378.14:004.056*

СИСТЕМА ПРАКТИКО-ОРИЕНТИРОВАННОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

А.А.ХОРЕВ

Федеральное государственное автономное образовательное учреждение
высшего образования «Национальный исследовательский университет
«Московский институт электронной техники»
г. Москва, 124498, Россия

Одним из важнейших направлений информационной безопасности является техническая защита информации, включающая защиту информации от несанкционированного доступа и программно-математических воздействий и защиту информации от утечки по техническим каналам.

К объектам технической защиты информации относятся объекты информатизации, на которых обрабатывается информация ограниченного доступа:

1. средства и системы информатизации различного назначения, обрабатывающие информацию ограниченного доступа;
2. б) помещения, предназначенные для ведения переговоров, содержащих информацию ограниченного доступа (далее – защищаемые помещения).

Защита этих объектов обеспечивается проведением организационных мероприятий и использованием технических, программных и программно-технических средств защиты информации.

С целью подтверждения соответствия объектов информатизации требованиям по защите информации проводится их аттестация.

Техническая защита информации в России является лицензируемым видом деятельности. Лицензирование данной деятельности осуществляет ФСТЭК России в соответствие с Постановлением правительства РФ от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» [1].

В России более 4060 организаций, являются лицензиатами ФСТЭК России, и оказывают услуги в области технической защиты информации [2].

Потребность в высококвалифицированных кадрах в области информационной безопасности и защиты информации постоянно растет, растут и контрольные цифры приема (см. табл. 1).

Таблица 1

Контрольные цифры приема по УГНПС 10.00.00 Информационная безопасность

Уровни высшего образования	2020	2021	2022	2023
Бакалавриат	2918	3647	3670	3707
Магистратура	808	663	742	777
Специалитет	3743	4344	4396	4536
Итого:	7469	8654	8808	9020

Перечень открытых федеральных государственных образовательных стандартов высшего образования по направлениям и специальностям в области информационной безопасности (ФГОС ВО), по которым осуществляется подготовка специалистов в области информационной безопасности, приведен в табл. 2.

Таблица 2

Направления и специальности подготовки по УГНПС 10.00.00 Информационная безопасность

Наименование ФГОС ВО		Приказ Минобрнауки России	Регистрация в Минюсте России	Квалификация
10.03.01	Информационная безопасность	№ 1427 от 17.11.2020	№62548 от 18.02.21	Бакалавр
10.04.01	Информационная безопасность	№ 1455 от 26.11.2020	№62549 от 18.02.21	Магистр
10.05.01	Компьютерная безопасность	№ 1459 от 26.11.2020	№62491 от 15.02.21	Специалист по защите информации
10.05.02	Информационная безопасность телекоммуникационных систем	№ 1458 от 26.11.2020	№62492 от 15.02.21	Специалист по защите информации

10.05.03	Информационная безопасность автоматизированных систем	№ 1457 от 26.11.2020	№62532 от 17.02.21	Специалист по защите информации
10.05.04	Информационно-аналитические системы безопасности	№ 1460 от 26.11.2020	№61702 от 22.12.20	Специалист по защите информации
10.05.05	Безопасность информационных технологий в правоохранительной сфере	№ 1461 от 26.11.2020	№61703 от 22.12.20	Специалист по защите информации

Однако, по данным рабочей группы на базе ВНИИ Труда Минтруда РФ, Ассоциации защиты информации (АЗИ), Федерального учебно-методического объединения в сфере высшего образования по УГСН 10.00.00 Информационная безопасность (ФУМО ИБ) более 30% работодателей не удовлетворены качеством подготовки специалистов в области защиты информации.

Одним из направлений повышения качества подготовки выпускников вузов в области защиты информации является реализация практико-ориентированного подхода, который основывается на реализации в рамках образовательной программы требований профессиональных стандартов в области информационной безопасности.

Основной особенностью новых ФГОС ВО является то, что универсальные и общепрофессиональные компетенции, формируемые у студентов, включены в федеральные государственные образовательные стандарты, а профессиональные компетенции определяются образовательной организацией самостоятельно на основе профессиональных стандартов (ПС), соответствующих профессиональной деятельности выпускников (рис.1).

В настоящее время приняты четыре открытых профессиональных стандарта (см. табл. 3) в области защиты информации и еще два находятся в стадии разработки: «Специалист по обеспечению безопасности значимых объектов критической информационной структуры» и «Специалист по криптографической защите информации».

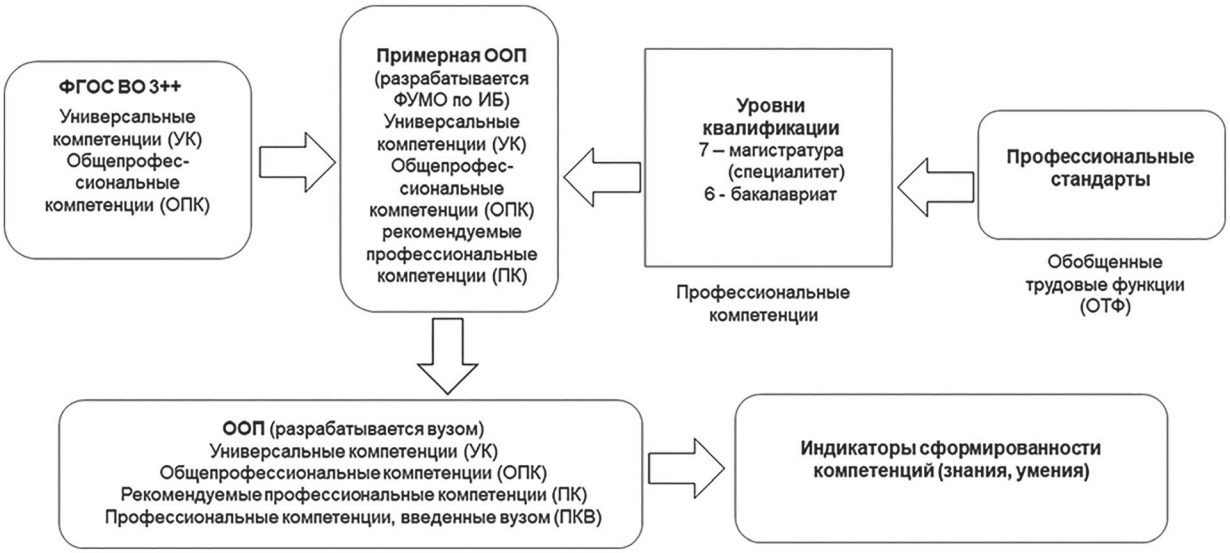


Рисунок 1. Особенности формирования профессиональных компетенций, в соответствии с требованиями ФГОС ВО

Таблица 3
Профессиональные стандарты в области защиты информации

Наименование профессионального стандарта	Дата утверждения
Специалист по защите информации в автоматизированных системах	Утвержден приказом Минтруда России 15.9.2016 № 522н
Специалист по технической защите информации	Утвержден приказом Минтруда России 01.11.2016 № 599н
Специалист по безопасности компьютерных систем и сетей	Утвержден приказом Минтруда России 01.11.2016 N 598н
Специалист по защите информации в телекоммуникационных системах и сетях	Утвержден приказом Минтруда России 03.11.2016 № 608н

Профессиональный стандарт является новой формой определения квалификации работника по сравнению с единым тарифно-квалификационным справочником работ и профессий рабочих и единым квалификационным справочником должностей руководителей, специалистов и служащих.

Профессиональный стандарт включает:

- общие сведения о виде профессиональной деятельности: наименование вида профессиональной деятельности и его место в структуре ОКВЭД;
- функциональную карту вида профессиональной деятельности: обобщенные трудовые функции (ОТФ), входящие в состав вида профессиональной деятельности: трудовые функции (ТФ), распределенные по квалификационным уровням;
- описание обобщенных трудовых функций: связь ОТФ с общероссийскими классификаторами, наименования возможных должностей; требования к образованию и обучению, требования к практическому опыту; описания трудовых функций, образующих ОТФ (трудовые действия, необходимые умения, необходимые знания).

То есть, профессиональный стандарт содержит перечень знаний и умений, необходимых для реализации трудовых функций, выполняемых в рамках соответствующей квалификации.

Пример перечня знаний и умений, необходимых для реализации трудовой функции «Проведение работ по установке, настройке и испытаниям защищенных технических средств обработки информации», уровень квалификации 6, в соответствие с требованием профессионального стандарта «Специалист по технической защите информации» приведен в табл. 4 [3].

Следовательно, образовательная организация, формируя профессиональные компетенции на основе трудовых функций, включенных в профессиональные стандарты соответствующих направлений профессиональной деятельности, должна включить в образовательную программу и индикаторы сформированности этих профессиональных компетенций (знания и умения).

Параллельно с разработкой профессиональных стандартов в России идет создание системы независимой оценки квалификации работников – процедуры подтверждения соответствия квалификации соискателя положениям профессионального стандарта (рис. 2).

Таблица 4

Перечень знаний и умений, необходимых для реализации трудовой функции «Проведение работ по установке, настройке и испытаниям защищенных технических средств обработки информации»

Необходимые умения	Производить установку и монтаж защищенных технических средств обработки информации
	Проводить настройку защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами
	Проводить испытания защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами
Необходимые знания	Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и эксплуатации защищенных технических средств обработки информации
	Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом «высокочастотного облучения» основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах
	Способы защиты информации от утечки по техническим каналам
	Технические средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок
	Методы и методики контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок
	Средства контроля эффективности мер защиты информации от утечки за счет побочных электромагнитных излучений и наводок
	Технические описания и инструкции по эксплуатации технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок
	Проектная документация на систему защиты объекта информатизации (в части защиты объекта от утечки информации за счет побочных электромагнитных излучений и наводок)
	Способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах
	Методы защиты информации от несанкционированного доступа и специальных программных воздействий на нее
	Программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее

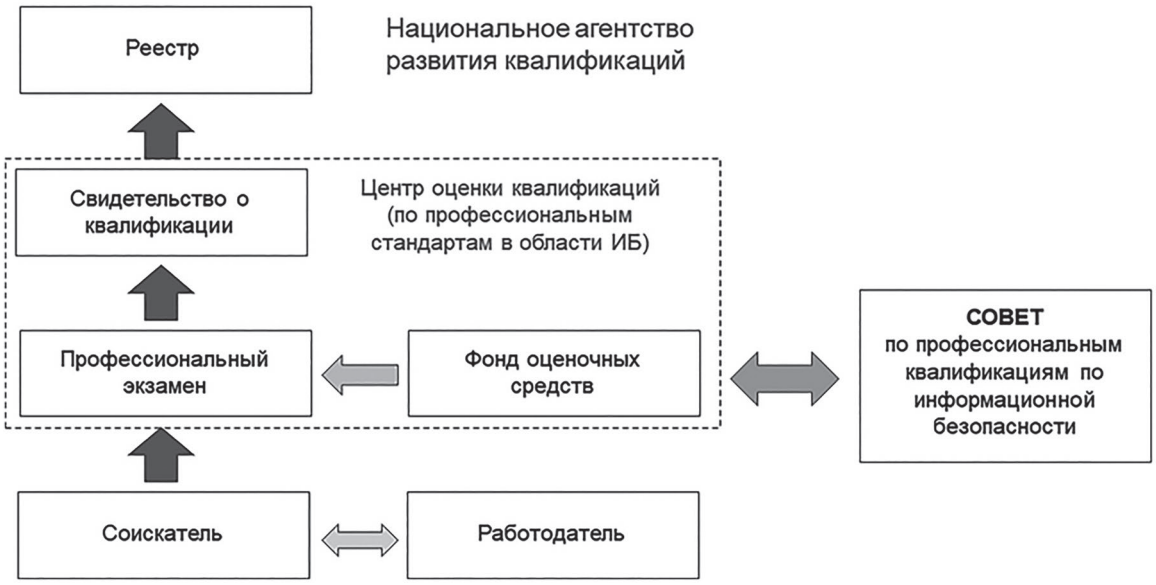


Рисунок 2. Система независимой оценки квалификации

Подтверждение квалификации осуществляется путем сдачи профессионального экзамена в центре оценки квалификации. Состав оценочных средств для проведения профессионального экзамена включает:

- вид профессиональной деятельности, профессиональный стандарт, наименование квалификации, уровень квалификации и номер квалификации;
- спецификацию заданий для теоретического этапа профессионального экзамена;
- спецификацию заданий для практического этапа профессионального экзамена;
- материально-техническое обеспечение оценочных мероприятий;
- кадровое обеспечение оценочных мероприятий;
- требования безопасности к проведению оценочных мероприятий;
- задания для теоретического этапа профессионального экзамена;
- задания для практического этапа профессионального экзамена;
- критерии оценки;
- правила обработки результатов профессионального экзамена и принятия решения о соответствии квалификации соискателя требованиям к квалификации;
- перечень нормативных правовых и иных документов, использованных при подготовке комплекта оценочных средств.

Порядок разработки и утверждения оценочных средств приведен на рис. 3.

Использование образовательной организацией для промежуточной аттестации оценочных средств, разработанных на основе оценочных средств, используемых при сдаче профессионального экзамена, позволит значительно повысить объективность оценки уровня подготовки выпускников различных вузов.

Одним из наиболее критичных показателей при организации сдачи профессионального экзамена, является наличие соответствующего материально-технического обеспечения оценочных мероприятий.

Например, для оценки профессиональной квалификации «Специалист по проведению работ по установке и техническому обслуживанию защищенных технических средств об-

Рисунок 3. Порядок разработки и утверждения оценочных средств для сдачи профессионального экзамена

работки информации» (6 уровень квалификации) материально-техническое обеспечение оценочных мероприятий должно включать:

1. материально-технические ресурсы для обеспечения теоретического этапа профессионального экзамена:
   помещение, площадью не менее 20 кв.м., оборудованное персональными компьютерами (с характеристиками не хуже: системный блок: процессор – Intel Core i5, количество ядер процессора 4, тактовая частота ядра – 3,4 ГГц, видеокарта – встроенная, графический процессор видеокарты – Intel, оперативная память – 8 ГГц, тип оперативной памяти - DDR4, объем жесткого диска SSD – 256 ГГб, интерфейсы – вход VGA, DisplayPort, HDMI, USB 3.0, сетевые интерфейсы - предустановленный модуль Wi-Fi (стандарт Wi-Fi 802.11 a/ac/b/g/n/ax), проводная сеть (LAN) - 10/100/1000 мбит/сек.;операционная система Microsoft Windows 10 Pro x64 Rus 1pk DSP OEI DVD; монитор 23,8» (IPS; 16:9; 250 cd/m2; 1000:1; 5ms; 1920x1080; 178/178; 2xHDMI; Tilt; Spk 2x5W, без мерцания; комплект (клавиатура+мышь; Microsoft Office 2013, Adobe Acrobat reader), подключенными к сети Интернет, письменными столами, стульями;
2. материально-технические ресурсы для обеспечения практического этапа профессионального экзамена: помещение, площадью не менее 20 кв.м., оборудованное:
   - письменными столами, стульями;
   - автоматизированными системами (АС) на базе персональных компьютеров, с характеристиками не хуже: системный блок: процессор – Intel Core i5, количество ядер процессора 4, тактовая частота ядра – 3,4 ГГц, видеокарта – встроенная, графический процессор видеокарты – Intel, оперативная память – 8 ГГц, тип оперативной памяти - DDR4, объем жесткого диска SSD – 256 ГГб, интерфейсы – вход VGA, DisplayPort, HDMI, USB 3.0, сетевые интерфейсы - предустановленный модуль Wi-Fi (стандарт Wi-Fi 802.11 a/ac/b/g/n/ax), проводная сеть (LAN) - 10/100/1000 мбит/сек.;операционная система Microsoft Windows 10 Pro x64 Rus 1pk DSP OEI DVD; монитор 23,8» (IPS; 16:9; 250 cd/m2; 1000:1; 5ms; 1920x1080; 178/178; 2xHDMI;

Tilt; Spk 2x5W, комплект (клавиатура+мышь; Microsoft Office, Adobe Acrobat reader), подключенными к сети Интернет;

- программно-аппаратными комплексами защиты АС от несанкционированного доступа к информации (типа Secret Net Studio);
- системами активной защиты от утечки информации по каналам побочных электромагнитных излучений и наводок (типа ЛГШ-503, Салют-3000Б, Соната-РС3 и др.);
- измерительный комплекс в составе анализатора спектра (типа FSL-3) и измерительной электрической антенны (типа НБА-02);
- средствами контроля защищенности информации (типа Ревизор 1 XP, Ревизор 2 XP, TERRIER, ФИКС, Ревизор Сети и др.).

В России 130 вузов реализуют образовательные программы в области информационной безопасности и защиты информации. Однако, немногие из них имеют современную учебно-материальную базу, необходимую для подготовки специалистов в области технической защиты информации и, в частности, в области защиты информации от утечки по техническим каналам.

Рассмотрим представленную выше модель практико-ориентированной подготовки специалистов в области технической защиты информации на примере подготовки бакалавров и магистров в НИУ МИЭТ.

Перечень профессиональных компетенций, формируемых у выпускников в области технической защиты информации, приведен в табл. 5.

В программе бакалавриата профессиональные компетенции, приведенные в табл. 5, формируются на основе профильных общепрофессиональных компетенций:

ОПК-3.1. Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам.

ОПК-3.2. Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа.

ОПК-3.3. Способен проводить контроль эффективности защиты информации от утечки по техническим каналам.

ОПК-3.4. Способен проводить контроль защищенности информации от несанкционированного доступа.

Формирование данных ОПК осуществляется в ходе изучения дисциплин: организационное и правовое обеспечение информационной безопасности, защита информации от несанкционированного доступа, программно-аппаратные средства защиты информации, основы построения и функционирования специальных технических средств, защита информации от утечки по техническим каналам, физическая защита объектов информатизации, основы управления информационной безопасностью, проектирование систем защиты объектов информатизации (деловая игра).

Формирование профессиональных компетенций происходит в ходе учебной (6 з.е.) и производственной (9 з.е.) практик, которые проводятся в 8-м семестре.

Цель учебной практики – получение первичных профессиональных умений и навыков. Практика проходит на базе кафедры «Информационная безопасность».

Цель производственной практики – получение профессиональных умений и опыта профессиональной деятельности. Практика проходит на базе НТЦ ТЗИ кафедры «Информационная безопасность» и ведущих предприятий г. Зеленограда и г. Москвы.

Таблица 5
Профессиональные компетенции, формируемые у выпускников НИУ МИЭТ, обучающихся по направлению «Информационная безопасность»

Направление направления подготовки	Код и наименование профессиональной компетенции выпускника	Трудовая функция из ПС, на основе которой сформулирована компетенция
10.03.01 Информационная безопасность (бакалавриат). Профиль «Техническая защита информации». Срок подготовки – 4 года	ПК-1. Способен проводить работы по установке, настройке и испытаниям защищенных технических средств обработки информации	B/6. Проведение работ по установке и техническому обслуживанию защищенных технических средств обработки информации. Уровень квалификации − 6.
	ПК-2. Способен проводить контроль эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок	D/02.6. Проведение контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок. Уровень квалификации − 6.
	ПК-3. Способен проводить контроль эффективности защиты акустической речевой информации от утечки по техническим каналам	D/03.6. Проведение контроля защищенности акустической речевой информации от утечки по техническим каналам. Уровень квалификации − 6
10.04.01 Информационная безопасность (магистратура. Программа «Аудит информационной безопасности» Срок подготовки – 2 года	ПК-1. Способен проводить аттестацию автоматизированных систем, средств обработки информации на соответствие требованиям безопасности информации	G/01.7. Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации. Уровень квалификации − 7.
	ПК-2. Способен проводить аттестацию выделенных (защищаемых) помещений на соответствие требованиям безопасности информации	G/02.7. Проведение аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации. Уровень квалификации − 7.

Производственная практика завершается выполнением 8-ми практико-ориентированных заданий, разработанных на основе оценочных средств, используемых при сдаче профессиональных экзаменов для оценки соответствующих профессиональных квалификаций.

В программе магистратуры профессиональные компетенции, приведенные в табл. 5, формируются при изучении дисциплин: технологии защиты информации от утечки по техническим каналам, технологии защиты информации от несанкционированного доступа, контроль защищенности информации от утечки по техническим каналам, правовые основы аудита информационной безопасности, организация аудита информационной безопас-

ности, оценка рисков информационной безопасности, аудит информационной безопасности автоматизированных систем (деловая игра), а таже в ходе производственной практики.

Производственная практика проходит в ходе 1-го (10 з.е.) и 2-го (12 з.е.) семестров. Цель практики – получение профессиональных умений и опыта профессиональной деятельности.

Практика проходит на базе проходит на базе НТЦ ТЗИ кафедры «Информационная безопасность» и ведущих предприятий г. Зеленограда и г. Москвы.

Заканчивается выполнением 8-ми практико-ориентированных заданий, разработанных на основе оценочных средств, используемых при сдаче профессиональных экзаменов для оценки соответствующих профессиональных квалификаций.

С целью формирования профессиональных компетенций на кафедре «Информационная безопасность» созданы четыре специализированные учебные лаборатории:

- лаборатория «Технологий и управления информационной безопасности»;
- лаборатория «Технологий и программно-аппаратных средств обеспечения информационной безопасности»;
- лаборатория «Технической защиты информации»;
- лаборатория «Специальных проверок и специальных исследований».

Лаборатории оснащены современной зарубежной и отечественной техникой и технологиями, позволяющими не только проводить лабораторные и практические занятия, но и научные исследования по различным направлениям технической защиты информации.

Список литературы

1. Постановление правительства РФ от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации». – URL: https://base.garant.ru/70136258/? (дата обращения: 08.06.2022).
2. Реестр лицензий на деятельность по технической защите конфиденциальной информации. – URL: https://fstec.ru/normotvorcheskaya/litsenzirovanie/72-reestry/216-reestr01 (дата обращения: 08.06.2022).
3. Приказ Минтруда России от 01.11.2016 N 599н «Об утверждении профессионального стандарта «Специалист по технической защите информации» (Зарегистрировано в Минюсте России 25.11.2016 № 44443). – URL: http://www.consultant.ru/document/cons_doc_LAW_207927/ (дата обращения: 08.06.2022).

ЗАОЧНЫЕ ДОКЛАДЫ

УДК 004.738.2

МЕТОДЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ СПЕЦИАЛИЗИРОВАННЫХ КОМПЕТЕНЦИЙ ПО СПЕЦИАЛЬНОСТИ ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИЯХ

Е.С. БЕЛОУСОВА, О.В. БОЙПРАВ, Т.В. БОРБОТЬКО
Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Беларусь

В рамках разработки образовательных стандартов и учебных планов в соответствии с решением Республиканского совета ректоров учреждений высшего образования о подготовке комплекта документов [1], обеспечивающих переход на стандарты высшего образования поколения 3+ были сформированы новые базовые профессиональные компетенции для выпускников разных специальностей.

В образовательном стандарте ОСВО 1-98 01 02-2021 и учебном плане специальности 1-98 01 02 «Защита информации в телекоммуникациях» среди множества компетенций выделим следующие:

- проектировать, настраивать и выполнять диагностику и администрирование локальных сетей передачи данных;
- применять принципы построения и защиты информации в волоконно-оптических системах передачи информации;
- нализировать, настраивать и проводить диагностику маршрутизации данных в IPv4 и IPv6 сетях;
- анализировать и устранять уязвимости в локальных сетях, настраивать коммутационное оборудование для противодействия кибератакам.

Представленные выше компетенции были определены на основе следующих требований, определенных в [1]:

- качество и конкурентоспособность образования;
- фундаментальность и актуальность содержания подготовки;
- связь с рынком труда и возможность оперативно реагировать на его запросы и др.

В [2] указано, что «при разработке учебных программ необходимо исходить из того, что их содержание должно обеспечить формирование компетенций, определенных учебными планами и образовательными стандартами высшего образования», а также «быть нацеленными на опережающую подготовку выпускников к решению задач инновационного экономического развития страны, предусматривать знакомство обучающихся с современными методами научных исследований и практикой применения новейших достижений науки, техники, культуры и производства».

В [3] проведено сравнение компетенций в CC Software Engineering и ОСВО l-40 01 01 «Программное обеспечение информационных технологий», на основе чего сделан вывод о высоких требованиях к уровню подготовки специалистов в области информаци-

онных технологий и необходимости приближения высшего образования к требованиям международных стандартов. Однако в данной работе приняты во внимание требований работодателей и зарубежных квалификационных систем для определения состава базовых профессиональных компетенций в таких областях знаний как основы компьютинга, проектирование программного обеспечения, эволюция программного обеспечения и др., но не защиты информации, которая является одним из обязательных требований для претендентов на работу.

Для формирования выше представленных компетенций в учебном плане специальности 1-98 01 02 «Защита информации в телекоммуникациях» утверждены следующие дисциплины: «Основы построения локальных сетей», «Маршрутизация в информационных сетях» и «Защита информационных сетей». Для совершенствования учебного процесса по данным дисциплинам будут использоваться методы обучения, предложенные И.Я. Лернером и М.Н. Скаткиным [4, 5], которые предложили пять методов обучения по типу и характеру познавательной деятельности, в каждом степень активности и самостоятельности в деятельности студентов нарастает.

В объяснительно-иллюстрированном методе студенты получают информацию и знания на лекциях, при подробном рассмотрении примеров топологий сетей и их конфигурации, которые так же присутствуют в учебно-методическом пособии [6].

Репродуктивный метод реализован в виде самостоятельного выполнения лабораторных работ и курсового проекта по дисциплине «Основы построения локальных сетей» с индивидуальным заданием, данный метод подразумевает последовательную конфигурацию определенных функции сетевого оборудования (коммутаторов, маршрутизаторов).

В ходе выполнения лабораторных работ часто студенты сталкиваются с методом проблемного изложения, когда ввиду совершения неточностей конфигурации сетевого оборудования возникают ошибки в передаче данных в локальных сетях. Такие ошибки обсуждаются на фронтальных занятиях с применением следующих активных методов обучения: дискуссии, моделирование конкретных ситуаций, кейс-метод, мозговая атака (штурм) и др., что позволяет развивать навыки мышления и реагирования в случае некорректной работы сетевого оборудования локальных сетей.

В ходе выполнения курсового проекта по дисциплине «Основы построения локальных сетей» студентам ставится задача проектирования локальной сети организации или, по-другому говоря, реализуется частично-поисковый (эвристический) метод, при котором студенты самостоятельно изучают различные виды оборудования, особенности их функционала, способов конфигурации, проектирования структурированной кабельной системы.

В рамках лабораторных работ по дисциплинам «Основы построения локальных сетей», «Маршрутизация в информационных сетях» и «Защита информационных сетей» и научно-исследовательской работы студентов (НИРС) реализуется исследовательский метод, посредством которого студенты изучают особенности содержания заголовков различных протоколов передачи данных в локальных сетях, анализируют уязвимости протоколов, эксплуатируют их, внедряют и разрабатывают меры по ликвидации этих уязвимостей, т.е. совершенствуют системы передачи данных для противодействия кибератакам. Результаты НИРС студенты представляют на различных конференциях и публикуют доклады в сборниках конференций [7–8]. Так, например, на 58-ой конференции аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет инфор-

матики и радиоэлектроники» были представлены доклады на темы, связанные с обеспечением аутентификации пользователей при доступе к беспроводной локальной сети, изучение принципов построения локальных сетей в симуляторах Cisco PT и eNSP с целью модернизации лабораторных работ по дисциплине «Основы построения локальных сетей» и «Защита информационных сетей».

Таким образом, с помощью методов обучения по типу и характеру познавательной деятельности, разработанных И.Я. Лернером и М.Н. Скаткиным, в рамках дисциплин «Основы построения локальных сетей», «Маршрутизация в информационных сетях» и «Защита информационных сетей» постепенно развиваются такие навыки студентов, как умение самостоятельно анализировать и устранять уязвимости в локальных сетях, разрабатывать и реализовывать методы по совершенствованию безопасности локальных сетей, быстро и своевременно реагировать на инциденты в корпоративных сетях и сбои работы сетевого оборудования. Так же необходимо отметить, что используемые методы обучения способствуют развитию самостоятельности приятия решений, совершенствованию в профессиональной деятельности, инициативе и адаптации к изменениям в профессиональной деятельности подготовленных студентов по специальности 1-98 01 02 «Защита информации в телекоммуникациях».

Список литературы

1. О разработке типовой учеб планирующей документации нового поколения (образовательных стандартов и примерных учебных планов) / Совет Ректоров Республики Беларусь, 2019-2020. URL: http://srrb.niks.by/wp-content/uploads/2019/12/2016-06-16-2.pdf (дата обращения: 21.04.2022).
2. Порядок разработки и утверждения учебных программ и программ практики для реализации содержания образовательных программ высшего образования / Белорусский государственный университет информатики и радиоэлектроники, 2002–2022. URL: https://www.bsuir.by/m/12_100229_1_138624.pdf (дата обращения: 21.04.2022).
3. Лапицкая Н.В., Шульдова, С.Г., Саркисян Г.Ф. К вопросу о разработке учебных планов поколения 3+ для специальности ИТ-профиля // Системный анализ и прикладная информатика. 2018. № 3. С. 70–75. URL: https://cyberleninka.ru/article/n/k-voprosu-o-razrabotke-uchebnyh-planov-pokoleniya-3-dlya-spetsialnosti-it-profilya. (дата обращения: 21.04.2022).
4. Лернер И. Я. Дидактические основы методов обучения. М. : Педагогика, 1981. 186 с.
5. Скаткин М. Н. Совершенствование процесса обучения. М. : Педагогика, 1971. 205 с.
6. Белоусова Е.С. Основы построения локальных сетей. Лабораторный практикум: учеб.-метод. пособие. Минск : БГУИР, 2020. 103 с.
7. Алейникова Д.И., Белоусова Е.С. Методы ликвидации коллизий при передаче данных в беспроводных сетях // 57-я конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 8 июня 2021 г., БГУИР, Минск, Беларусь: тезисы докладов. Мн. 2021. С. 7–8.
8. Кондрашук О.А., Белоусова Е.С. Проблемы безопасности интернета вещей // Современные средства связи : материалы XXVI Междунар. науч.-техн. конф., 21–22 окт. 2021 года, Минск, Респ. Беларусь. Минск : Белорусская государственная академия связи, 2021. С. 58–60.

УДК 004.05

ПОДХОДЫ К УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЯХ НА ОСНОВЕ ТРЕБОВАНИЙ РЕГУЛЯТОРОВ

Е.А. БЕЛЯЕВ, И.И. ЛИВШИЦ
Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»,
г. Санкт-Петербург, 197101, Российская Федерация

Введение

Развитие организаций банковской системы Российской Федерации напрямую связано с состоянием информационной безопасности. Важнейшей задачей обеспечения информационной безопасности в кредитно-финансовых учреждениях является минимизация рисков информационной безопасности и предотвращения последствий реализации угроз и снижение ущерба, который может быть нанесен организации.

Организации кредитно-финансовой сферы находятся в зоне весьма сложного регулирования. Ввиду критичности обрабатываемой внутри организаций информации, кредитно-финансовые организаций вынуждены выполнять требования различных регуляторов (ФСТЭК, ФСБ, Банк России) по информационной безопасности. Требования регуляторов регулярно пересматриваются, наслаиваясь друг на друга, зачастую не имеют четких и формализованных методик. Учитывая коммерческую направленность деятельности, кредитно-финансовые организации на ряду с необходимостью выполнить требования всех регуляторов стремятся оптимизировать расходы на информационную безопасность.

В рамках системы управления информационной безопасностью в организациях банковской системы весомую роль играет оценка соответсвия информационной безопасности кредитно-финансовой сферы требованиям Банка России. Этот инструмент при его грамотном применении позволяет достичь соотвествующего баланса для организации системы защиты информации и определения бюджета кредитно-финансовой организации на обеспечение информационной безопасности. В случае, если кредитно-финансовые организации проводят указанную процедуру осознано, а не с формальной точки зрения только лишь для направления отчета в Банк России, то указанный инструмент позволяет определять уязвимые места в системе менеджмента информационной безопасности, выстроенной внутри банка. Результаты оценки позволяют точечно вносить изменения в систему защиты организации, совершенствовать ее, исключая избыточные меры защиты и усиливая обеспечение информационной безопасности в направлениях, в которых зафиксированы уязвимые зоны.

Банком России разработаны соответствующие документы, регламентирующие порядок проведения оценки соответствия кредитно-финансовых организаций требованиям информационной безопасности, умелое применение которых позволит достигнуть оптимального уровня информационной безопасности и расходов на ее обеспечение.

1. Оценка соответствия кредитно-финансовых организаций требованиям по информационной безопасности в соответствии с комплектом стандартов Банка России по обеспечению информационной безопасности СТО БР ИББС.

Банком России разработан и регулярно актуализируется комплект документов СТО БР ИББС, который по состоянию на текущий момент включает в себя 8 стандартов и 8 рекомендаций по стандартизации. Указанный набор стандартов определяет рекомендации регулятора к системе обеспечения информационной безопасности организаций банковской системы. Внедрение СТО БР ИББС стало драйвером развития информационной безопасности российской финансовой отрасли и позволило повысить стабильность всей банковской системы Российской Федерации.

В соответствии с требованиями законодательства Российской Федерации для указанного комплекта стандартов установлен рекомендательный статус. При этом следует отметить, что стандарты и иные документы по стандартизации подлежат обязательному исполнению в организациях, если они добровольно принимают решение о присоединении.

Таким образом, указанный комплект документов не является прямым указанием кредитно-финансовым организациям к действиям, при этом банки могут самостоятельно принять решение о присоединении к СТО БР ИББС.

Анализ документов, входящих в состав СТО БР ИББС позволяет установить, что при его разработке используются лучшие мировые практики из признанных эффективными стандартов и рекомендаций по информационной безопасности. На достаточно длительный промежуток времени, указанный комплект стал весьма эффективным инструментом для построения системы управления информационной безопасности в кредитно-финансовых организациях

Один из документов стандарта (СТО БР ИББС-1.2-2014. Дата введения: 2014-06-01) определяет методику оценки соответствия информационной безопасности организации банковской системы Российской Федерации.

Организациям кредитно-финансовой сферы, присоединившимся к Комплексу СТО БР ИББС рекомендуется проходить внешнюю оценку соответствия требованиям СТО БР ИББС-1.0 с периодичностью раз в два года.

Процедура оценки производится на основе частных и групповых показателей информационной безопасности. Групповые показатели вычисляются на основе частных как среднее арифметическое. На основе групповых показателей вычисляются итоговые показатели по трем направлениям: текущий уровень информационной безопасности, менеджмент информационной безопасности и уровень осознания информационной безопасности. Также отдельно вычисляются уровни соответствия по защите персональных данных.

Значения всех полученных групповых показателей ИБ отображаются на круговой диаграмме соответствия, что позволяет визуализировать состояние информационной безопасности по каждому оцениваемому направлению, а также отслеживать динамику изменений уровней оценки в зависимости от года проведения аудита при наложении результатов оценки на диаграмму.

2. Оценка соответствия кредитно-финансовых организаций требованиям по информационной безопасности в соответствии с ГОСТ Р 57580.2-2018. НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Безопасность финансовых (банковских) операций. ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ. Методика оценки соответствия.

В целях закрепления обязательных требований к обеспечению информационной безопасности в кредитных организациях был разработан и внедрен стандарт Безопасность финансовых (банковских) операций, состоящий из двух частей ГОСТ Р 57580.1-2017 и ГОСТ Р 57580.2-2018, первый документ содержит базовый набор организационных и технических мер по обеспечению ИБ, второй документ определяет методику оценки соответствия стандарту. Документы определяют три уровня защиты информации.

Проведение оценки соответствия в соответствии с требованиями стандарта осуществляется с привлечением стороннего аудитора, лицензированного ФСТЭК. Регламент проведения оценки (градацию, формулы для подсчета итоговых оценок, форму и порядок предоставления отчетности в Банк России) определен в ГОСТ Р 57580.2-2018.

В стандарте вводится понятие операционного риска, что является отсылкой к международным требованиям и основанным на них требованиям, введенным Банка России. Так документом[18] Базель III Базельского комитета по банковскому надзору, членом которого является Российская Федерация, определены требования к управлению кредитным и операционным рисками. Несмотря на то, что документ косвенно затрагивает риски информационной безопасности, он играет важное значение для выработки унифицированного подхода к управлению различными типами рисков. Центральный банк Российской Федерации установил требования к системе управления операционным рисков в Положении Банка России от 08.04.2020 г. № 716-П[19]. Указанное положение определяет требование к ведению баз данных о событии операционного риска, в том числе риска информационной безопасности.

В соответствии со стандартом осуществляется оценка соответствия по следующим требования:

1. Обеспечение защиты информации при управлении доступом;
2. Обеспечение защиты вычислительных сетей;
3. Контроль целостности и защищенности информационной инфраструктуры;
4. Защита от вредоносного кода;
5. Предотвращение утечек информации;
6. Управление инцидентами защиты информации;
7. Защита среды виртуализации;
8. Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств.

---

[18] Basel III: A global regulatory framework for more resilient banks and banking systems, Bank for International Settlements 2010

[19] Положении Банка России от 08.04.2020 г. № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

3. Синтез подходов к оценке соответствия кредитных организации требованиями СТО БР ИББС и ГОСТ Р 57580.2-2018.

Исходя из результатов проведенного анализа, оценка соответствия кредитно-финансовой организации носит обязательный характер, а применение комплекта СТО БР ИИБС является обязательным только при добровольном присоединении кредитной организации к выполнению комплекта стандартов.

Указанное дублирование стандартов создает сложности для финансовых организаций при принятии решений о способах проведения оценки соответствия. При этом, как было сказано ранее, оба документа являются полезными инструментами для кредитной организации при реализации и совершенствовании системы управления информационной безопасности. Синтез указанных методик позволит обеспечить наиболее оптимальный подход к обеспечению информационной безопасности в кредитных организациях.

Также необходимо учитывать, что кредитные организации подпадают под требования законодательства в части критической информационной инфраструктуры. С учетом стремительно меняющейся обстановки на мировой арене и возникновении острой потребности в реализации импортозамещения в сфере информационной безопасности кредитно-финансовых организаций требования по уровню соответствия кредитно-финансовой организации возможно будут пересматриваться регуляторами.

Заключение

1. Ф**изический процесс, генерируемый источником случайности на основе шумового диода,** является недостаточно стационарным.
2. Частоты встречаемости отсчетов достаточно симметрично распределены относительно математического ожидания и имеют одну моду. При этом не удалось подтвердить гипотезу о нормальном распределении на приемлемом уровне значимости.
3. Наличие марковской зависимости с применением байесовского информационного критерия (BIC) не выявлено.
4. Вероятности отсчетов согласуются с гипотезой о равновероятном распределении четных и нечетных отсчетов. Следовательно, в выходных бинарных последовательностях распределение 0 и 1 также будет близко к равновероятному.

Список литературы

1. ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер [Текст]. –введен 01 января 2018 г. – М.: Стандартинформ, 2018.
2. ГОСТ Р 57580.2-2018 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия [Текст]. –введен 01 сентября 2018 г. – М.: Стандартинформ, 2018.
3. Беляев Е.А., Емельянова О.А., Лившиц И.И. Анализ методик оценки рисков информационной безопасности кредитно-финансовых организаций. Научно-технический вестник информационных технологий, механики и оптики [Scientific and Technical Journal of Information Technologies, Mechanics and Optics]. 2021. Т. 21. № 3(133). С. 437-441.
4. Стандарт Банка России СТО БР ИББС-1.2-2014. «Обеспечение безопасности организаций системы Российской Методика оценки соответствия информационной безопасности организации банковской системы Российской Федерации» –– 2014 г.

УДК 004.056

АНАЛИЗ ВЕКТОРОВ ПОТЕНЦИАЛЬНЫХ АТАК НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ ОРГАНИЗАЦИЙ ЭЛЕКТРОСВЯЗИ

В.А. БОЙПРАВ, Л.Л. УТИН
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»
г. Минск, *220013,* Республика Беларусь

В настоящее время практически все предприятия и организации используют услуги доступа к сетям электросвязи в рамках своих бизнес-процессов: для эффективного поиска или предоставления информации, пользования ресурсами электронной почты, осуществления банковских операций, построения систем электронного документооборота. Даже небольшие перерывы в связи, вызванные сбоями в работе аппаратуры, повреждениями в линиях передачи и другими причинами приводят к прямым и косвенным затратам, срывам выгодных контрактов и потери репутации. Ввиду изложенного информационные системы (ИС), используемые в организациях электросвязи для предоставления услуг, относятся к критически важным объектам информации и одним из основных национальных интересов Республики Беларусь в информационной сфере является обеспечение надежности и устойчивости функционирования таких объектов [1].

Наиболее серьезная причина снижения надежности и устойчивости функционирования сетей электросвязи обусловлена угрозами информационной безопасности, направленными на ИС, используемые в организациях электросвязи для предоставления услуг. Следовательно, построение систем защиты информации для таких ИС, а также обеспечение эффективности их функционирования и эксплуатации направлены на поддержание национальных интересов как Республики Беларусь, так и Российской Федерации в информационной сфере. Указанные процессы сопряжены с созданием системы менеджмента информационной безопасности (СМИБ), а непрерывность совершенствования последней – с проведением ее аудита [2]. В соответствии с изложенным, можно отметить, что аудит СМИБ организаций электросвязи является одним из основополагающих процессов в обеспечении надежности и устойчивости функционирования сетей электросвязи.

Согласно [3], одним из ключевых этапов аудита СМИБ является анализ полученных результатов. По мнению авторов, наиболее трудоемкий процесс из всех процессов, связанных в совокупности с реализацией этого этапа, заключается в анализе векторов потенциальных атак на ИС аудируемой организации.

Авторами предложено в ходе анализа векторов атак на ИС использовать следующие классификационные признаки:

1. объект воздействия;
2. характер реализации;
3. продолжительность реализации;
4. путь реализации.

В зависимости от первого классификационного признака можно выделить следующие разновидности атак на ИС:

- атаки, направленные на аппаратные средства ИС;
- атаки, направленные на программные (аппаратно-программные) средства ИС;
- атаки, направленные на информационные технологии, реализуемые в ИС;
- атаки, направленные на информационные ресурсы.

В зависимости от второго классификационного признака можно выделить следующие разновидности атак на ИС:

- случайные;
- целенаправленные.

В зависимости от третьего классификационного признака можно выделить следующие разновидности атак на ИС:

- быстрые;
- медленные.

В зависимости от четвертого классификационного признака можно выделить следующие разновидности атак на ИС:

- реализуемые непосредственно (т. е. путем физического доступа);
- реализуемые опосредованно:
- локально (через локальную сеть)
- удаленно (через смежную или глобальную сеть).

Следует отметить, что, как правило, случайные атаки являются быстрыми, а целенаправленные – медленными.

Случайная и быстрая атака может включать в себя следующие этапы:

1. разведка;
2. подготовка ресурсов;
3. доставка;
4. эксплуатация;
5. установка;
6. управление и контроль;
7. воздействие.

Процесс реализации целенаправленной и медленной атаки, как правило, включает в себя два дополнительных этапа по сравнению с процессом реализации случайной и быстрой атака. Такими этапами являются проектирование и предотвращение обнаружения. Наличие этапа проектирования в рамках атаки рассматриваемого типа основывается на том факте, что в ходе ее реализации нарушители информационной безопасности стремятся собрать как можно больше информации об объекте воздействия из социальной среды или других источников до момента подготовки ресурсов. Наличие этапа предотвращения обнаружения в рамках атаки рассматриваемого типа основывается на том факте, что нарушители информационной безопасности стремятся оставаться незамеченным с той целью, чтобы усложнить для пользователей атакованной ИС идентификацию атаки.

Следовательно, целенаправленная и медленная атака включает в себя следующие этапы:

1. проектирование;
2. разведка;
3. подготовка ресурсов;
4. доставка;
5. эксплуатация;
6. предотвращение обнаружения;
7. установка;

8. управление и контроль;
9. воздействие.

В совокупности причисленные этапы атак каждого из типов представляют собой вектор атаки.

В работе [4] определено, что в настоящее время наиболее вероятными атаками, направленными на ИС организаций электросвязи, используемые для предоставления услуг (телекоммуникационные системы в соответствии с прямым переводом текста указанной работы) являются следующие:

- системная инсайдерская атака;
- DDoS-атака;
- сканирование портов;
- атака по бэкдор-каналу;
- атака, направленная на получение root-прав;
- атака на виртуальную машину или гипервизор.

В таблице 1 представлен результат анализа векторов указанных атак с использованием предложенных авторами классификационных признаков.

Таблица 1

Результат анализа векторов потенциальных атак на ИС организаций электросвязи, используемые для предоставления услуг

Наименование атаки	Характер реализации	Продолжительность реализации	Объект воздействия	Путь реализации
Системная инсайдерская атака	Целенаправ-ленные	Медленная	Аппаратные средства, программные (аппаратно-программные) средства, информаци-онные технологии, информаци-онные ресурсы	Непосредственно (физический доступ)
DDoS-атака	Целенаправленные	Медленная	Информационные технологии	Опосредованно удаленно (через смежную или глобальную сеть)
Сканирование портов	Целенаправленная	Медленная	Программные средства	Опосредованно удаленно (через смежную или глобальную сеть)
Атака по бэкдор-каналу	Целенаправленная	Медленная	Программные средства	Опосредованно удаленно (через смежную или глобальную сеть)

Атака, направленная на получение root-прав	Целенаправленная	Медленная	Программные средства	Опосредованно удаленно (через смежную или глобальную сеть)
Атака на виртуальную машину или гипервизор	Целенаправленная	Медленная	Программные средства	Опосредованно удаленно (через смежную или глобальную сеть)

Таким образом, на основе результатов проведенного анализа было установлено, что в настоящее время вектора потенциальных атак на ИС организаций электросвязи, используемые для предоставления услуг, чаще всего направлены на программные средства и реализуются опосредованно удаленно (через смежную или глобальную сеть).

Список литературы

1. Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575 « Об утверждении Концепции национальной безопасности Республики Беларусь» // Нац. реестр правовых актов Респ. Беларусь. – 2010. – № 276. – 1/12080. – 21 с.
2. Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководящие положения по проведению аудита систем менеджмента информационной безопасности: ISO/IEC 27007:2020 ; введ. 21.01.2020. – Минск: Госстандарт Республики Беларусь, 2020. – 46 с.
3. Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководящие положения по проведению аудита систем менеджмента информационной безопасности : ISO/IEC 27007:2020 ; введ. 21.01.2020. – Минск : Госстандарт Республики Беларусь, 2020. – 46 с.
4. Japertas S., Baksys T. Method of Early Staged Cyber Attacks Detection in IT and Telecommunication Networks // Elektronika ir elektrotechnika. 2018. Vol. 24, No. 3. P. 68–77.

УДК 004.915

РАЗРАБОТКА ЭЛЕКТРОННОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА ПО ДИСЦИПЛИНЕ «ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ», СОДЕРЖАЩЕГО ВИДЕОЛЕКЦИИ

О.В. БОЙПРАВ, Е.С. БЕЛОУСОВА, Г.А. ПУХИР
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»
г. Минск, *220013,* Республика Беларусь

В Республике Беларусь дисциплина «Основы защиты информации» является одной из дисциплин, составляющих основу подготовки специалистов с высшим образованием и относится к циклу общепрофессиональных или специальных дисциплин. В связи с этим представляется целесообразным создать условия для повышения эффективности освое-

ния студентами материалов указанной дисциплины. Один из наиболее часто применяемых в настоящее время подходов, направленных на повышение эффективности образовательного процесса, основан на использовании в рамках последнего видеолекций [1].

Выделяются следующие преимущества использования видеолекций в образовательном процессе, обуславливающие повышения эффективности последнего, которая определяется уровнем усвоения обучающимися материалов учебных дисциплин, а также удовлетворенностью обучающихся обозначенным процессом:

1. обеспечение для обучающихся возможности самостоятельного управления темпом усвоения материала, которое реализуется путем выбора одного из следующих режимов просмотра видеолекции [1]:
   - непрерывный режим без повторного просмотра видеолекции;
   - непрерывный режим с повторным просмотром всей видеолекции;
   - непрерывный режим с повторным просмотром отдельных фрагментов видеолекции;
   - режим с прерываниями видеолекции на отдельных ее фрагментах с целью их повторного просмотра;
2. обеспечение для обучающихся возможности закрепления обсуждавшегося на лекции материала при подготовке к сдаче зачета или экзамена.
3. обеспечение для преподавателя возможности использования активных методов обучения в ходе проведения лекционных занятий, в частности:
   - организация лекции с использованием метода «перевернутый класс»;
   - организация лекции-дискуссии;
   - организация лекции-консультации;
   - организация проблемной лекции;
   - проведение контрольных опросов во время аудиторного лекционного занятия, составленных на основе материалов видеолекций и направленных на определение тех их тем, в усвоении которых у обучающихся возникли наибольшие трудности;

В связи с обозначенными преимуществами авторами был разработан электронный образовательный ресурс (ЭОР) по дисциплине «Основы защиты информации», содержащий видеолекции, наряду с текстовым и иллюстративным материалом. В ходе подготовки указанного ЭОР авторами совместно со специалистами Центра развития дистанционного образования было поочередно реализованы следующие шаги.

1. Разбиение материалов дисциплины на модули. В результате реализации этого шага все материалы лекционных и практических занятий по дисциплине были распределены по четырем модулям:
   - Модуль 1. Техническая защита информации;
   - Модуль 2. Криптографическая защита информации;
   - Модуль 3. Организационные аспекты управления интеллектуальной собственностью;
   - Модуль 4. Правовые аспекты управления интеллектуальной собственностью.
2. Определение тем занятий, для которых представляется целесообразным разработка видеолекций. В ходе реализации этого шага авторы опирались на личный опыт преподавания дисциплины «Основы защиты информации» для студентов специальностей технико-технологического и экономического профилей учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», в частности, на знаниях о том, в усвоении материалов каких из тем указанной дисциплины

у студентов возникают наибольшие трудности. Было установлено, что таковыми темами являются следующие:

- «Методология информационной безопасности» (далее по тексту – тема 1);
- «Классификация технических каналов утечки информации по физическим принципам возникновения» (далее по тексту – тема 2);
- «Управление доступом в информационных системах» (далее по тексту – тема 3);
- «Криптосистемы» (далее по тексту – тема 4);
- «Понятие и принципы авторского права» (далее по тексту – тема 5);
- «Объекты промышленной собственности» (далее по тексту – тема 6);
- «Коммерческое использование объектов интеллектуальной собственности» (далее по тексту – тема 7);
- «Судебная экспертиза объектов интеллектуальной собственности» (далее по тексту – тема 8).

Темы 1 и 2 относятся к Модулю 1, темы 3 и 4, темы 5 и 6, темы 7 и 8 – соответственно к Модулям 2, 3, 4.

3. Написание сценариев для видеолекций. В ходе реализации этого шага авторы руководствовались следующими требованиями к содержанию эффективных видеолекций (т. е. видеолекций, в результате внедрения которых в образовательный процесс должно быть обеспечено повышение уровня усвоения обучающимися материалов учебных дисциплин по сравнению с уровнем усвоения материалов аналогичных дисциплин, наблюдавшимся до момента такого внедрения) [2]:
   - монотемность (содержание видеолекции должно быть связано с раскрытием сути одного вопроса);
   - модульность (содержание видеолекции должно представлять собой «завершенный блок дидактически адаптированной информации» [3]);
   - содержание видеолекции должно быть раскрыто в течение не более чем 15 минут.

   Результатом реализации рассматриваемого шага стали 14 сценариев для видеолекций, содержание каждой из которых было связано с раскрытием сути одного из вопросов, относящихся к темам 1–8 дисциплины.
4. Студийная съемка и монтаж видеолекций. В ходе реализации данного шага учитывались следующие требования, предъявляемые к оформлению видеолекций:
   - наличие видеоизображения лектора в большинстве кадров видеолекции (иными словами – обеспечение персонификации фигуры лектора);
   - наличие спецэффектов в тех фрагментах видеолекции, на которых нужно заострить внимание обучающихся в наибольшей степени.

Обозначенные требования были обусловлены результатами исследования эффективности видеолекций различного содержания, представленными в работе [4]. Следует отметить, что эти исследования базировались на получении закономерностей динамики тета- и альфа-ритмов в электроэнцефалографии человека в зависимости от его функционального состояния, а именно, в зависимости от содержания просматриваемой им видеолекции (видеолекция, содержащая слайды, анимационные вставки, графическое и текстовое отражение информации / видеолекция, содержащая видеоизображение лектора).

В таблице 1 представлены сведения о разработанных в результате реализации рассматриваемого шага видеолекций.

Таблица 1. Сведения о разработанных видеолекциях

Тема дисциплины, с которой связана видеолекция	Тема видеолекции	Продолжительность видеолекции
Тема 1	Что такое защита информации?	5 минут
	Классификация информации	5 минут
	Классификация угроз информационной безопасности	6 минут
Тема 2	Классификация технических каналов утечки информации по физическим принципам возникновения	15 минут
Тема 3	Управление доступом в информационных системах	13 минут
Тема 4	Основы построения криптосистем	11 минут
	Электронная цифровая подпись	6 минут
Тема 5	Понятие и принципы авторского права	14 минут
Тема 6	Группы объектов промышленной собственности	2,5 минуты
	Изобретения, полезные модели, промышленные образцы	10,5 минут
	Товарные знаки, знаки обслуживания и географические указания	4 минуты
	Секреты производства	5 минут
Тема 7	Коммерческое использование объектов интеллектуальной собственности	14 минут
Тема 8	Судебная экспертиза объектов интеллектуальной собственности	15 минут

Рисунок 1. Кадр видеолекции по теме «Классификация технических каналов утечки информации по физическим принципам возникновения»

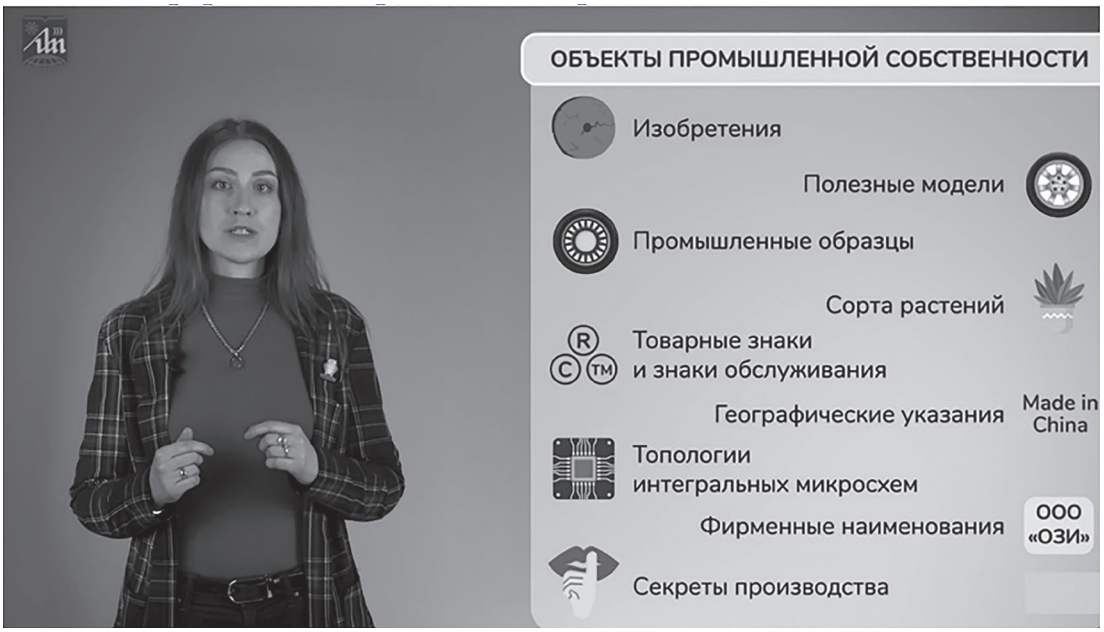


Рисунок 2. Кадр видеолекции по теме «Группы объектов промышленной собственности»

Исходя из сведений, представленных в таблице 1, можно заключить, что видеолекции отвечают требованиям, предъявляемым к их содержанию. Рисунки 1 и 2 являются подтверждением того, что разработанные видеолекции также отвечают требованиям, предъявляемым к их оформлению.

Разработанный авторами ЭОР по дисциплине «Основы защиты информации» в настоящее время используется преподавателями кафедры защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» в ходе проведения практических занятий по обозначенной дисциплине. Кроме того, этот ЭОР задействуется в рамках реализуемого на базе указанного учреждения образования экспериментального проекта, направленного на оценку эффективности смешанного обучения.

Список литературы

1. Кулиева О.Н. Об эффективности использования обучающих видео в преподавании // Идеи. Поиски. Решения: сборник статей и тезисов XIII Международной научно-практической конференции преподавателей, аспирантов, магистрантов, студентов. – Минск, 22 ноября 2019 г. Минск: БГУ, 2020. – С. 17–22.
2. Серов В.Н. Основные концепции создания видеолекций для электронного учебника // Сборник научных трудов «Дистанционные образовательные технологии». – М.: ТГУ: 2004. – С. 240–242.
3. Природова О.Ф., Никишина В.Б. Модульные видеолекции: оценка эффективности // Коллекция гуманитарных исследований. Электронный научный журнал. – 2017. – № 4 (7). – С. 17–23.
4. Лазаренко В.А., Природова О.Ф., Никишина В.Б., Кузнецова А.А. Технология оценки эффективности видеолекции // Профессиональное образование в России и за рубежом. – 2018. – № 1 (29). – С. 45–52.
5.

УДК 004.056.5

ПРОБЛЕМЫ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ФЕДЕРАЛЬНОГО ЗАКОНА № 187 «О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ» ОТ 26 ИЮЛЯ 2017 ГОДА

О. А. КОПЫРУЛИНА
Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»,
г. Санкт-Петербург, 190000, Россия

Введение

Проблема реализации требований 187-ФЗ на данный момент актуальна и широко обсуждаема, 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 объектов критической информационной инфраструктуры. Согласно данной статье показатель 2 и 3 категории объектов критической информационной инфраструктуры не может быть определен корректно, исходя из границ их значений. Авторы предлагают изменить последовательность этапов категорирования объектов критической информационной инфраструктуры и первым этапом сделать составление перечня объектов критической информационной инфраструктуры, подлежащих категорированию. Смена этапов обуславливается тем, что в комиссию по категорированию нужно включать только осведомленных специалистов [1]. Данная позиция достаточно интересна, однако возникает вопрос: если комиссия не назначена, кто будет уполномочен в правильном составлении перечня объектов критической информационной инфраструктуры?

В статье Котова А.А, Куринной В.С, Шлыкова М.С «Алгоритм категорирования объектов критической информационной инфраструктуры» рассматривается проблема алгоритмизации процесса категорирования объектов критической информационной инфраструктуры. Авторы предлагают алгоритм, согласно которому значительно снижаются затраты на категорирование объектов критической информационной инфраструктуры. 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 объектов критической информационной инфраструктуры металлургических предприятий. Автор предлагает автоматизировать часть процесса категорирования объектов критической информационной инфраструктуры [3]. 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 критической информационной инфраструктуры сталкиваются со следующими проблемами:

- отсутствие методик ФСТЭК России по категорированию объектов критической информационной инфраструктуры;
- избыточность и сложность процедур, требуемых для выполнения постановления правительства №127;
- действия нарушителей в отношении объектов критической информационной инфраструктуры, угрозы безопасности информации и уязвимости никак не влияют на итоговую категорию;
- нестабильность требований постановления правительства №127 и приказов ФСТЭК России.

1.1. Отсутствие методик ФСТЭК России по категорированию ОКИИ

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 критической информационной инфраструктуры исходя из сферы деятельности субъекта, но идентифицировать однозначно объекты критической информационной инфраструктуры 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 критической информационной инфраструктуры?
- многие организации, попадающие под перечень сфер, пользуются услугами подрядчиков и не имеют собственных информационных систем, как быть в этом случае?
- также стоит учитывать во внимание организации не осуществляющие свою деятельность в указанных сферах, но имеющие информационные системы, функционирующие в указанных сферах деятельности, являются ли они значимыми объектами критической информационной инфраструктуры?

В форму уведомления и в реестр значимых объектов критической информационной инфраструктуры вносится информация исключительно по сферам деятельности объекта критической информационной инфраструктуры, а не субъекта.

1.2. Избыточность и сложность процедур, требуемых для выполнения постановления правительства №127

На основании Федерального закона №187 [4] можно сделать выводы, что категорирование объектов критической информационной инфраструктуры - это ничто иное как соответствие объектов критической информационной инфраструктуры критериям значимости и показателям, присвоение объекту одной из категорий значимости, а также проверку ре-

зультатов присвоения. В постановлении правительства №127 [5] введены дополнительные обязанности для субъекта критической информационной инфраструктуры, усложняющие определение категорий значимости, но не оказывающие влияние на итоговую категорию.

Таким образом появляется следующие противоречие: субъект критической информационной инфраструктуры обязан вначале выявить объекты критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, но ФЗ-187 указывает, что обязательно категорирование всех без исключения объектов критической информационной инфраструктуры.

Также в постановлении правительства №127 [5] существует формулировка о необходимости согласования перечня объектов критической информационной инфраструктуры с государственным органом или российским юридическим лицом, которая зачастую воспринимается субъектом критической информационной инфраструктуры 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 критической информационной инфраструктуры перечней объектов критической информационной инфраструктуры не предусмотрена. Это приводит к низкой эффективности процедуры согласования перечней объектов критической информационной инфраструктуры и большим временным потерям на служебную переписку между организациями и подведомственными им субъектами критической информационной инфраструктуры.

Также документы по результатам категорирования (акт и форма уведомления о результатах категорирования) дублируют друг друга.

1.3. Действия нарушителей в отношении объектов критической информационной инфраструктуры, угрозы безопасности информации и уязвимости никак не влияют на итоговую категорию.

Согласно ПП 127 субъект критической информационной инфраструктуры обязан провести анализ возможных действий нарушителей в отношении объектов критической информационной инфраструктуры, угроз безопасности информации и уязвимостей, которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры. При этом результаты проведенного анализа никак не используются при установлении каждому из объектов критической информационной инфраструктуры одной из категорий значимости либо принятии решения об отсутствии необходимости присвоения категорий значимости [5].

Таким образом, значимый объект критической информационной инфраструктуры может быть недостаточно защищен от действий злоумышленников или же наоборот, некоторые меры защиты могут быть излишне, что повлечет за собой необоснованные расходы.

1.4. Нестабильность требований постановления правительства №127 и приказов ФСТЭК России

Изначально редакция постановления правительства №127 [5] содержала ошибки в нескольких показателях критериев значимости.

На текущий момент ФСТЭК России решила не просто исправить ошибки в постановлении правительства №127 [5], а внести радикальные изменения в процессы категорирования: изменены принципы создания и расформирования комиссии по категорированию субъекта критической информационной инфраструктуры, радикально занижены пороговые показа-

тели 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.

Для усовершенствования процесса категорирования необходимо:

1. Исключить избыточные этапы, не оказывающие влияния на определение показателей категорий значимости объектов критической информационной инфраструктуры:
   - составление перечня объектов, подлежащих категорированию, и последующих действий с ним.
2. Этап оформления акта категорирования объекта критической информационной инфраструктуры заменить на заполнение формы уведомления о результатах категорирования.
3. Создать единую методику категорирования и программное обеспечение для автоматизации процесса категорирования, учитывая влияние действий нарушителей в отношении объектов критической информационной инфраструктуры, угроз безопасности информации и уязвимостей на итоговую категорию значимости.

Заключение

Проблема реализации требований 187-ФЗ на данный момент актуальна и широко обсуждаема, так как отсутствует практически опыт реализации нормативных требований, а также изданные нормативно-правовые акты проработаны не до конца.

На практике субъекты критической информационной инфраструктуры сталкиваются со следующими проблемами:

- отсутствие методик ФСТЭК России по категорированию объектов критической информационной инфраструктуры;
- избыточность и сложность процедур, требуемых для выполнения постановления правительства №127;
- действия нарушителей в отношении объектов критической информационной инфраструктуры, угрозы безопасности информации и уязвимости никак не влияют на итоговую категорию;
- нестабильность требований постановления правительства №127 и приказов ФСТЭК России.

Данные проблемы могут решаться путем создания единой методики по категорированию объектов критической информационной инфраструктуры, которая будет исключать избыточные этапы, не оказывающие влияния на определение категории значимости объектов критической информационной инфраструктуры. Этап оформления акта категорирования объекта критической информационной инфраструктуры может быть заменен на заполнение формы уведомления о результатах категорирования. Также должно учитываться влияние действий нарушителя в отношении объектов критической информационной инфраструктуры, угроз безопасности информации уязвимостей на итоговую категорию значимости.

Список литературы

1. 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.

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. 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 учёных (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.
4. Федеральный Закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 № 187-ФЗ // Российская газета. 2017 г..
5. 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.

УДК 577.3.043

ВЛИЯНИЕ ЭЛЕКТРОМАГНИТНЫХ ШУМОВЫХ ИЗЛУЧЕНИЙ НА ЭМОЦИОНАЛЬНОЕ СОСТОЯНИЕ ОПЕРАТОРА

А.В. СИДОРЕНКО, Н. А. СОЛОДУХО
Белорусский государственный университет
Минск, 220030, Республика Беларусь

Актуальной в настоящее время становится проблема обеспечения информационной безопасности в различных сферах деятельности человека, в том числе, предупреждения искажения информации либо несанкционированного к ней доступа. При этом предъявляются повышенные требования как к безопасности циркулирующей информации, так и к обеспечению защищенности человека от техногенных излучений, стрессов и других факторов воздействия [1, 2].

Широкое распространение информационных технологий, методов обработки и анализа сложных сигналов способствуют более точной оценке реакций центральной нервной системы при воздействии электромагнитных шумовых излучений или измененных ее состояниях, Существенное значение приобретают вопросы обеспечения стабильности эмоционального состояния человека, работающего в условиях необходимости быстрого принятия решений, в том числе, в мобильных (передвижных) системах. При этом особое внимание уделяется оценке работоспособности человека, что при наличии состояния стресса, депрессии, умственной усталости проявляется временной неспособностью выполнять когнитивные действия, в силу трудностей с концентрацией внимания и, соответственно, необходимостью пролонгации временных рамок для принятия решения.

В работе проводятся исследования экспериментально полученных в клинических условиях паттернов электроэнцефалограмм человека в условиях электромагнитных шумовых излучений и результаты сравнительного анализа с паттернами при депрессии, стрессе.

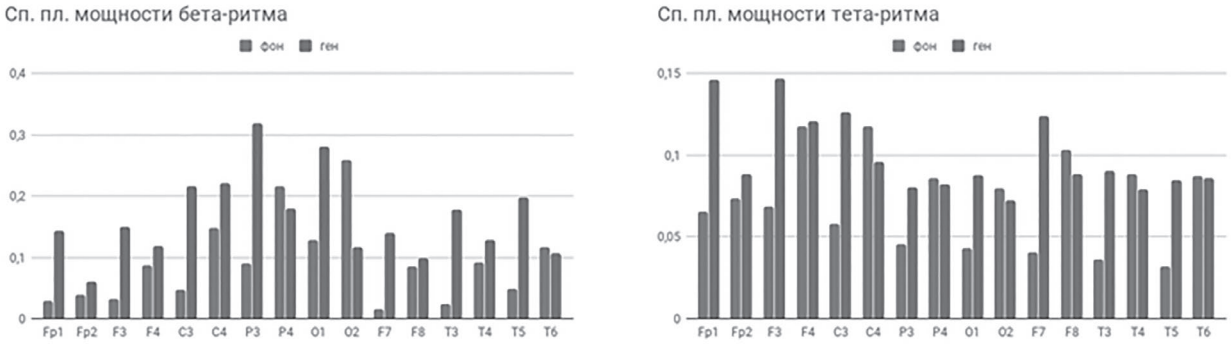
2. Методика проведения исследований

Регистрация электроэнцефалограмм осуществлялась по Международной схеме “10/20” с использованием электроэнцефалографа “Нейрокартограф“. Погрешность измерения электроэнцефалографа составляет 5 %. Обработка и анализ электроэнцефалограмм проводились в разработанной нами информационно-измерительной системе, адаптированной для работы с электроэнцефалограммами [3]. Электроэнцефалограммы обрабатывались в следующих режимах: фон, наличие генератора шумового электромагнитного излучения. В режиме: фон использовались электроэнцефалограммы здорового человека .

Спектральная плотность мощности ритмов головного мозга рассчитывалась с помощью быстрого преобразования Фурье. Анализируемые диапазоны ритмических составляющих включали: альфа-ритм (8-12) Гц, бета-ритм (12-20) Гц, тета-ритм (4-8) Гц, гамма-ритм (20-40) Гц. Параметры нелинейного анализа: выборочная энтропия, корреляционная размерность, фрактальная размерность, сложность Лемпеля-Зива рассчитывались согласно алгоритмам, приведенным в работах [3, 4, 5, 6] .

3. Результаты и их обсуждение

Депрессия. Рассмотрим вопросы синхронизации и десинхронизации бета- и тета-ритмов между левым и правым полушариями головного мозга при действии шумового излучения (рис. 1).



а) б)

Рисунок1. Гистограммы распределений спектральной плотности мощности бета-ритма (а) и тета-ритма (б) электроэнцефалограмм под действием шума

При изучении поведения бета-ритма наблюдается десинхронизация в электроэнцефалограммах трех пар отведений (P3 и P4; O1 и O2; T5 и T6) - т. е. в электроэнцефалограммах левого полушария отмечается возрастание бета-ритма относительно фона, а в правом – уменьшение. При рассмотрении тета-ритма наблюдается десинхронизация между левым и правым полушарием у электроэнцефалограмм шести пар отведений (C3 и C4; P3 и P4; O1 и O2; F7 и F8; T3 и T4; T5 и T6) – т. е. в левом полушарии головного мозга наблюдается возрастание тета-ритма, а в правом – его уменьшение. Суммарно, в электроэнцефалограммах

16 пар отведений для бета- и тета-ритмов наблюдается больше пар с рассинхронизацией ритмов (девять пар), чем с синхронизацией (семь пар), что может являться следствием скрытой депрессии у оператора, как это описано в работе [6].

Проанализируем изменения фрактальной размерности в восьми отведениях Fp1, Fp2, T3, T4, P3, P4, O1, O2 (рис. 2) электроэнцефалограмм оператора.

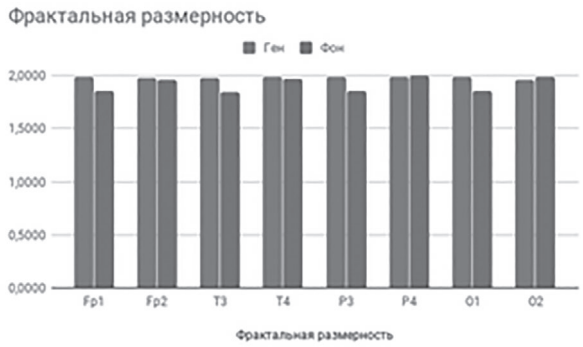


Рисунок 2. Гистограммы распределения фрактальной размерности электроэнцефалограмм при электромагнитном шуме

Вариации фрактальной размерности в электроэнцефалограммах относительно фона сводятся к следующему: наблюдается возрастание фрактальной размерности в электроэнцефалограммах в условиях шума в шести из восьми анализируемых отведений Fp1, Fp2, T3, T4, P3, O1. Возрастание фрактальной размерности в электроэнцефалограммах отведений Fp1, Fp2, T3, T4, P3, P4, O1, O2 является признаком депрессии, как это отмечается в работе [7]. Следовательно, можно заключить, что оператор в условиях действия электромагнитного шумового излучения находится в состоянии депрессии.

Проанализируем изменения параметра выборочной энтропии в электроэнцефалограммах отведений Fp1 и T3: при наличии электромагнитного шумового излучения она возрастает в 2,8 раза в отведении Fp1 относительно фона и в четыре раза – в отведении T3 (рис. 3).

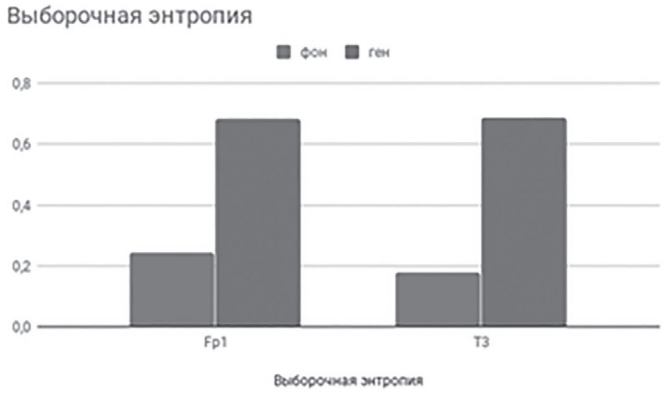


Рисунок 3. Гистограммы распределения выборочной энтропии электроэнцефалограмм в отведениях Fp1, T3 при действии генератора шума

Параметр выборочной энтропии также возрастает в электроэнцефалограммах отведений Fp1, T3 относительно фонового значения [4], что позволяет сделать вывод о том, что при наличии генератора шума оператор находится в состоянии депрессии.

Анализ динамики параметров: спектральной плотности мощности бета-, тета-ритмов, фрактальной размерности, выборочной энтропии позволяет сделать вывод, что оператор под действием электромагнитного шума испытывает депрессию.

Стресс. Рассмотрим изменение параметров электроэнцефалограмм человека, связанных со стрессом. В условиях электромагнитного шумового излучения наблюдается возрастание спектральной плотности мощности бета-ритма в электроэнцефалограммах отведений Fp1, Fp2, Fpz в пять раз от фона, на 56,1 % от фона, и в 2,5 раза от фона, соответственно (рис.4).

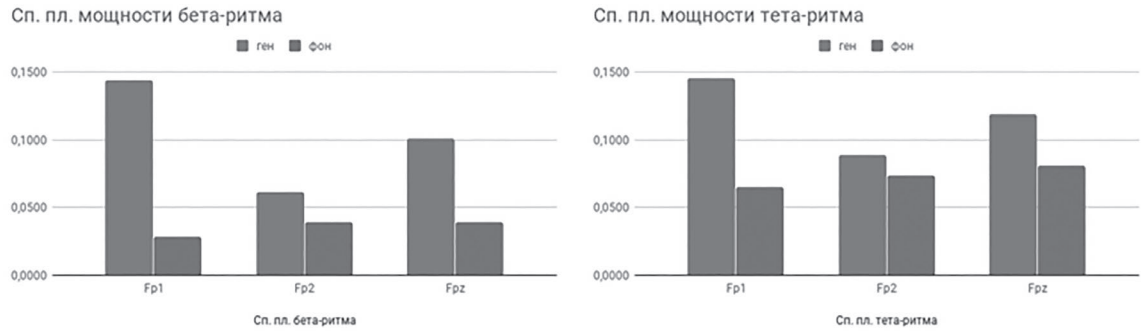


Рисунок 4. Гистограммы распределения спектральной плотности мощности бета-ритма электроэнцефалограмм в отведениях Fp1, Fp2, Fpz при действии шума

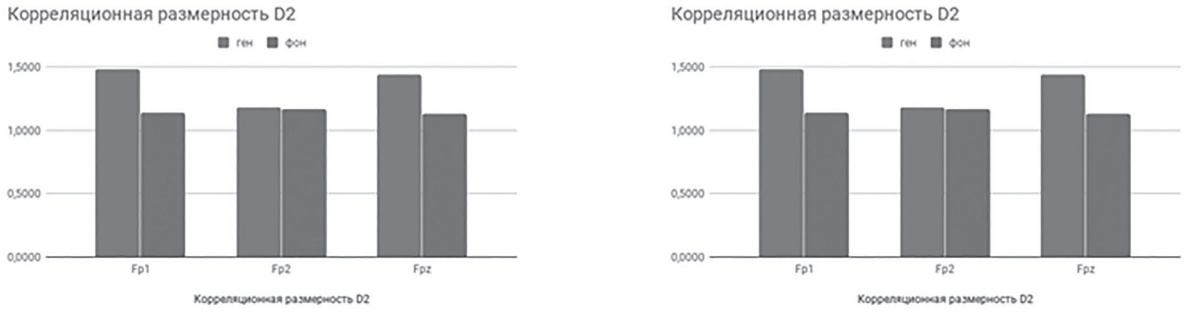
Это может быть признаком стресса, так как на основе материла, приведенного в работе [8], в состоянии стресса возрастает спектральная плотность мощности бета-ритма в электроэнцефалограммах отведений Fp1, Fpz.

При действии генератора шума у оператора также наблюдается возрастание спектральной плотности мощности тета-ритма в электроэнцефалограммах отведений Fp1, Fp2, Fpz: в 2,2 раза от фона, на 20,8 % от фона, и на 47,4 % от фона, соответственно. Это может быть признаком наличия стресса, так как из материала, представленного в работе [8], следует, что при стрессе у человека возрастает спектральная плотность мощности тета-ритма в электроэнцефалограммах отведений Fp1, Fp2, Fpz.

Следует отметить, что при проведении исследований электроэнцефалограмм отмечаются также вариации нелинейных параметров: корреляционной размерности и сложности Лемпела-Зива. В отведениях Fp1, Fp2, Fpz при наличии генератора шума наблюдается увеличение параметра корреляционной размерности на 30,7 % от фона, на 0,9 % от фона, и на 27,6 % от фона, соответственно, (рис. 5)

Подобные изменения параметра корреляционной размерности являются характерными для состояния стресса, как это отмечается в работе [8], поэтому можно сделать вывод, что оператор испытывает стресс.

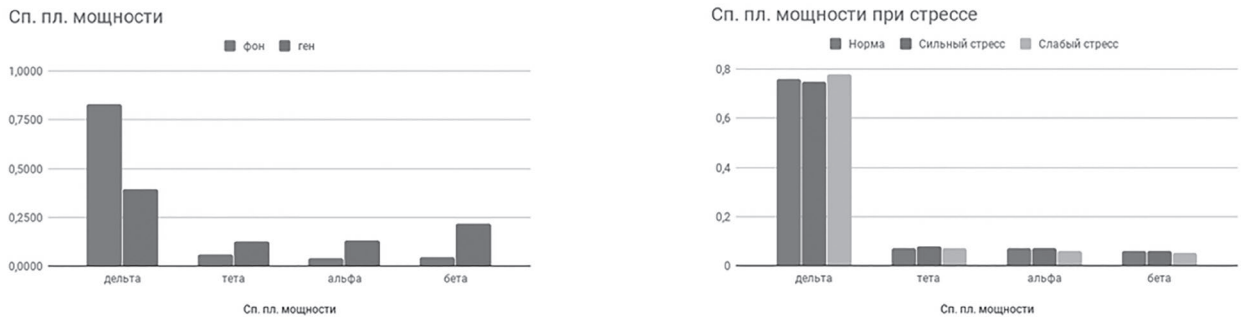
В процессе проведенного нами эксперимента под действием генератора шума наблюдается возрастание параметра сложности Лемпела Зива в электроэнцефалограммах отведений Fp1, Fp2, Fpz в 5,3 раза от фона, в 4,7 раза от фона, и в 6 раз от фона, соответственно (рис.5 б)). Так как при стрессе наблюдается возрастание сложности Лемпела-Зива в рассмотренных выше отведениях, то можно сделать вывод, что в условиях электромагнитного шумового излучения оператор находится в состоянии стресса.



а) б)

Рисунок 5. Гистограммы распределения корреляционной размерности (а), сложности Лемпела-Зива (б) электроэнцефалограмм при действии шума

Исходя из выявленных в процессе эксперимента изменений спектральной плотности мощности в электроэнцефалограмме отведения С3 (рис. 6) (спектральная плотность мощности дельта- ритма снизилась в 2,1 раза относительно фона; тета-ритма –возросла в 2,2 раза, альфа-ритма увеличилась в 3,3, бета-ритма возросла в 4,5 раза) в условиях шума (а именно, из уменьшения спектральной плотности мощности дельта-ритма и возрастания спектральных плотностей мощности тета-, альфа- и бета-ритмов), а также приведенной в работе [9] информации, можно заключить, что оператор испытывает сильный стресс.



а) б)

Рисунок 6. Гистограммы распределения спектральной плотности мощности электроэнцефалограмм в отведении С3 : а- под действием электромагнитного шума, б- в состоянии стресса [9]

В состоянии стресса у человека также как и при действии электромагнитного шума снижается спектральная плотность мощности дельта-ритма и возрастает спектральная плотность мощности тета-ритма в отведении С3 электроэнцефалограммы. Для данного отведения уровень альфа- и бета-ритмов можно исключить из анализа, так как при сильном стрессе они не изменяются.

Полученные результаты показывают, что при действии электромагнитного шума согласно анализу паттернов электроэнцефалограмм оператор испытывает стресс.

3. Заключение

В результате проведенных нами экспериментальных исследований паттернов электроэнцефалограмм установлено, что в условиях электромагнитного шумового излучения оператор, принимающий, обрабатывающий и передающий информацию, и находящийся в мобильной системе, испытывает состояние депрессии, стресса, что становится особенно важным при необходимости быстрого принятия решений.

Список литературы

1. Сидоренко, А.В., Солодухо Н.А. Воздействие шумового излучения на центральную нервную систему. Электроника ИНФО. 2016;(11):58-62.
2. Сидоренко А.В., Солодухо Н.А. Эмоциональное состояние оператора при воздействии электромагнитного шумового излучения. Доклады БГУИР. 2019;(4):5-10.
3. Сидоренко, А.В. Методы информационного анализа биоэлектрических сигналов. Мн.: БГУ; 2003.
4. Richman J.S., Moorman J.R. Physiological time-series analysis using approximate entropy and sample entropy. Am. J. Physiol. Heart Circ. Physiol. 2000;278(6):2039–2049.
5. Harne B.P. Higuchi Fractal Dimension Analysis of EEG Signal before and after OM Chanting to Observe Overall Effect on Brain. IJECE. 2014;4(4):585-592.
6. Armitage R., Hoffman R.F., Rush A.J. Biological rhythm disturbance in depression: temporal coherence of ultradian sleep EEG rhythms. Psychol Med. 1999;29(6):1435-1448.
7. Bachmann M. Spectral Asymmetry and Higuchi's Fractal Dimension Measures of Depression Electroencephalogram. Computational and Mathematical Methods in Medicine. 2013;2013:251638-1-251638-8.
8. Hong Peng, A method of identifying chronic stress by EEG. Personal and Ubiquitous Computing. 2013;17(17):1341–1347.
9. Perrin S.L. Waking qEEG to assess psychophysiological stress and alertness during simulated on-call conditions. International Journal of Psychophysiology. 2019;141:93-100.

УДК 621.383

ПРОПУСКНАЯ СПОСОБНОСТЬ КВАНТОВО-КРИПТОГРАФИЧЕСКОГО КАНАЛА СВЯЗИ

А. М. ТИМОФЕЕВ
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Введение

Одной из важнейших задач в сфере информационной безопасности объектов критической информационной инфраструктуры является обеспечение скрытности и конфиденциальности передаваемой информации [1]. Данными объектами могут быть, например, секретные криптографические ключи. Эти ключи часто требуется распределять по открытым каналам связи, к которым может иметь доступ злоумышленник.

Для решения указанных задач, как правило, применяют комплекс мер, включая использование квантово-криптографических каналов связи. Это позволяет достичь абсолютной скрытности и конфиденциальности передаваемой информации за счет ее кодирования посредством квантово-механического ресурса [2]. При этом обмен информацией осуществляется посредством маломощных оптических импульсов, содержащих не более десяти фотонов в расчете на каждый бит (символ). Регистрация таких сигналов возможна с помощью высокочувствительных приемных моделей, в качестве которых достаточно часто применяют счетчики фотонов [3].

Однако счетчик фотонов ввиду неидеальности своих технико-эксплуатационных характеристик могут приводить к ошибкам при регистрации данных. Одной из причин таких ошибок может являться ненулевое мертвое время счетчика фотонов – это время, в течение которого приемный модуль не чувствителен к падающему на него оптическому излучению [2, 3]. В результате возникают так называемые «просчеты».

Под просчетом понимается событие, когда на вход счетчика фотонов поступает фотон регистрируемого излучения, однако на его выходе фотон не регистрируется.

В свою очередь, «просчеты» приводят к снижению одной из достаточно важных характеристик квантово-криптографических каналов связи – пропускной способности, которая определяется максимальной скоростью передачи информации [4].

В известных литературных источниках отсутствует оценка влияния скорости счета сигнальных импульсов на выходе счетчика фотонов с мертвым временем на пропускную способность квантово-криптографического канала связи. Целью данной работы являлось выполнение такой оценки.

Объектом исследования являлся асинхронный двоичный несимметричный однородный квантово-криптографический канал связи без памяти и со стиранием, содержащий в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа. Выбор в качестве объекта исследования такого канала связи обусловлен тем, что его использование не требует наличия дополнительных линий связи для передачи и приема синхроимпульсов [5, 6]. Мертвым временем продлевающегося типа характеризуются счетчики фотонов на базе лавинных фотоприемников, включенных по схеме пассивного гашения лавины [3].

Предметом исследования являлось установить влияние средней длительности мертвого времени продлевающегося типа на пропускную способность квантово-криптографического канала связи.

1. Выражение для оценки пропускной способности квантово-криптографического канала связи. Дальнейшие рассуждения будут основаны на том, что квантово-криптографический канал связи выполнен с использованием приемо-передающий устройств [7]. Математическая модель этого канала связи построена в работе [4].

Для оценки пропускной способности квантово-криптографического канала связи воспользуемся выражением [4]:

$$\begin{aligned} C_{\max} = \{ & -\left[0{,}5\left(P(0/0)+P(0/1)\right)\right]\times\log_2\left[0{,}5\left(P(0/0)+P(0/1)\right)\right] - \\ & -\left[0{,}5\left(P(1/0)+P(1/1)\right)\right]\times\log_2\left[0{,}5\left(P(1/0)+P(1/1)\right)\right] - \\ & -\left[0{,}5\left(P(-/0)+P(-/1)\right)\right]\times\log_2\left[0{,}5\left(P(-/0)+P(-/1)\right)\right] + \\ & +0{,}5\left[P(0/0)\log_2 P(0/0)+P(1/0)\times\log_2 P(1/0)+P(-/0)\log_2 P(-/0)\right] + \\ & +0{,}5\left[P(0/1)\log_2 P(0/1)+P(1/1)\log_2 P(1/1)+P(-/1)\log_2 P(-/1)\right]\}/\tau_b, \end{aligned} \quad (1)$$

где $P(0/0)$ и $P(0/1)$ – вероятности регистрации на выходе канала связи символа «0» при наличии на его входе символов «0» и «1» соответственно, $P(1/0)$ и $P(1/1)$ – вероятности регистрации на выходе канала связи символа «1» при наличии на его входе символов «0» и «1» соответственно, $P(-/0)$ и $P(-/1)$ – вероятности того, что на выходе канала связи не будет зарегистрирован ни символ «0», ни символ «1» при наличии на его входе символов «0» и «1» соответственно; τ_b – среднее время передачи одного бита (символа).

Переходные вероятности $P(0/0)$, $P(-/0)$, $P(1/0)$, $P(0/1)$, $P(-/1)$ и $P(1/1)$, входящие в формулу (1), можно определить на основании статистических распределений числа импульсов на выходе счетчика фотонов по методике [8]:

$$P(0/0)=\sum_{N=N_1}^{N_2}\frac{\left[(n_t+n_{s0})(\Delta t-\tau_d)\right]^N\exp\left[-(n_t+n_{s0})(\Delta t-\tau_d)\right]}{N!}, \quad (2)$$

$$P(-/0)=\sum_{N=0}^{N_1-1}\frac{\left[(n_t+n_{s0})(\Delta t-\tau_d)\right]^N\exp\left[-(n_t+n_{s0})(\Delta t-\tau_d)\right]}{N!}, \quad (3)$$

$$P(1/0)=1-P(0/0)-P(-/0), \quad (4)$$

(5)

$$P(0/1)=\sum_{N=N_1}^{N_2}\frac{\left[(n_t+n_{s1})(\Delta t-\tau_d)\right]^N\exp\left[-(n_t+n_{s1})(\Delta t-\tau_d)\right]}{N!}, \quad (6)$$

$$P(1/1)=1-P(0/1)-P(-/1), \quad (7)$$

N_1 и N_2 – нижний и верхний пороговые уровни регистрации соответственно, n_t – средняя скорость счета темновых импульсов на выходе счетчика фотонов, n_{s0} и n_{s1} – средние скорости счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «0» и «1» соответственно, Δt – среднее время однофотонной передачи, τ_d – средняя длительность мертвого времени продлевающегося типа.

Нижний и верхний пороговые уровни регистрации – это соответственно наименьшее и наибольшее число зарегистрированных на выходе счетчика фотонов импульсов, при котором делается вывод, что передан символ «0». При превышении зарегистрированных импульсов числа N_2 делается вывод, что передан символ «1», а при регистрации импульсов в количестве, меньшем, чем N_1, принимается решение, что символ отсутствует [4, 7].

Темновые и сигнальные – это импульсы, которые появляются на выходе счетчика фотонов соответственно в отсутствии оптического сигнала и в результате воздействия фотонов регистрируемого излучения [3].

Отметим, что для оценки мертвого времени продлевающегося типа используют среднее значение, поскольку его длительность зависит от интенсивности оптического излучения [3].

Таким образом, для оценки пропускной способности рассматриваемого канала связи необходимо в формулу (1) подставить соответствующие выражения (2) ÷ (7) при заданных пороговых уровнях регистрации N_1 и N_2, скоростях счета импульсов n_t, n_{s0} и n_{s1} и длительностях Δt и τ_d.

2 Результаты математического моделирования и их обсуждение. Вычисление пропускной способности выполнялось для квантово-криптографических каналов связи, содержащих в качестве приемного модуля счетчик фотонов при различных значениях n_{s0} и n_{s1} при отсутствии мертвого времени продлевающегося типа, а также при его наличии.

На рисунке 1 представлены зависимости пропускной способности квантово-криптографического канала связи от средней скорости счета сигнальных импульсов при передаче двоичных символов «1» при отсутствии мертвого времени продлевающегося типа, а также при его наличии.

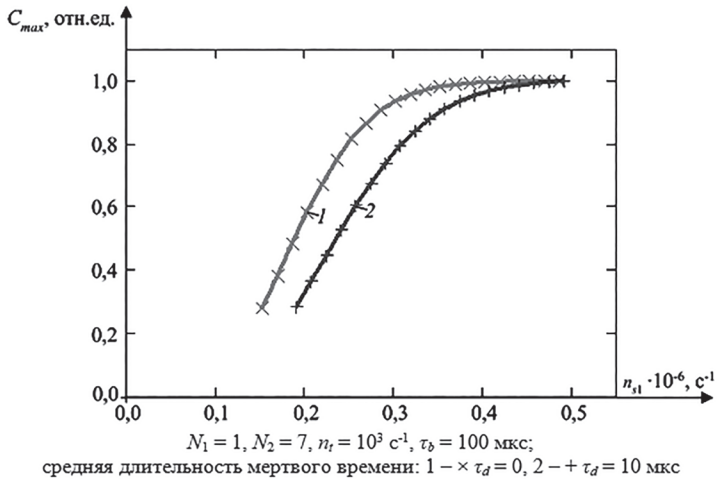


Рисунок 1. Зависимости пропускной способности канала связи от средней скорости счета сигнальных импульсов при передаче двоичных символов «1»

Все графики нормированы на величину $1/\tau_b$. Зависимости $C_{\max}(n_{s1})$ построены в диапазонах средних скоростей счета сигнальных импульсов n_{s1}, на которых переходные вероятности $P(1/1) \geq 0{,}5$ при заданных средних длительностях мертвого времени продлевающегося типа. Это обусловлено тем, что для рассматриваемого канала связи при $P(1/1) < 0{,}5$ использование счетчиков фотонов для регистрации данных становится нецелесообразным. Оценка переходных вероятностей $P(1/1)$ выполнялась по методике [6]. Для сравнения полученных зависимостей $C_{\max}(n_{s1})$ величины средних скоростей счета сигнальных импульсов n_{s0} фиксировались постоянными и выбирались по методике [5]. Расчет проводился для одинаковых значений нижнего и верхнего пороговых уровней регистрации $N_1 = 1$ и $N_2 = 7$, средней скорости счета темновых импульсов $n_t = 10^3$ с$^{-1}$ и среднего времени передачи одного бита (символа) $\tau_b = 100$ мкс. Необходимо также отметить, что пороговые уровни регистрации можно выбирать и другими, отличными от 1 и 7, но при сравнении зависимостей $C_{\max}(n_{s1})$ для различных средних длительностей мертвого времени N_1 и N_2 следует фиксировать постоянными, как и среднее значение скорости счета темновых импульсов n_t и среднее время передачи одного бита (символа) τ_b [5, 6]. Отметим, что при других значениях N_1, N_2 и отношениях $\tau_d/\Delta t$, n_t/n_{s0} и n_t/n_{s1} проявление эффекта мертвого времени продлевающегося типа аналогично представленному на рисунке 1.

Как видно из полученных результатов, с ростом средней скорости счета сигнальных импульсов при передаче двоичных символов «1» пропускная способность канала связи увеличивается вплоть до насыщения, что наблюдается как при наличии мертвого времени продлевающегося типа (см. рисунок 1, кривая 2), так и при его отсутствии (см. рисунок 1, кривая 1). Причем при прочих равных параметрах увеличение средней длительности мертвого времени продлевающегося типа приводит к тому, что насыщение зависимостей $C_{\max}(n_{s1})$ наблюдается при более высоких значениях n_{s1}: при $n_{s1} \geq 35{,}0 \times 10^4$ с$^{-1}$ для $\tau_d = 0$; при $n_{s1} \geq 43{,}7 \times 10^4$ с$^{-1}$ для $\tau_d = 10$ мкс. Такие особенности поведения зависимостей $C_{\max}(n_{s1})$ объ-

ясняются характером изменения достоверности принятых данных D с увеличением средних скоростей счета сигнальных импульсов n_{s1} и средней длительности мертвого времени продлевающегося типа [6].

Под достоверностью будем понимать вероятность того, что принятые данные соответствуют переданным [6].

В исследуемых диапазонах значений средних скоростей счета сигнальных импульсов с увеличением n_{s1} достоверность принятых данных D также увеличивается, достигая насыщения. Повышение достоверности принятых данных D приводит к снижению условной энтропии $H(B/A)$ и к росту пропускной способности исследуемого канала связи. Это объясняется следующим. При наименьших значениях средних скоростей счета сигнальных импульсов в случае передачи двоичных символов «1» для исследуемых диапазонов n_{s1} максимумы статистических распределений смеси числа темновых и сигнальных импульсов на выходе счетчика фотонов при регистрации символов «1» $P_{st1}(N)$ находятся между нижним N_1 и верхним N_2 пороговыми уровнями регистрации. При этом вероятность того, что на выходе канала связи будет зарегистрирован символ «0», в то время, когда на вход канала связи подается символа «1», максимальна. В этом случае переходная вероятность $P(0/1)$ также максимальна, что, в свою очередь, не позволяет достигать наибольшего значения переходной вероятности $P(1/1)$. С увеличением n_{s1} происходит сдвиг максимумов статистических распределений $P_{st1}(N)$ в сторону больших значений N, поэтому увеличивается вероятность регистрации на выходе счетчика фотонов импульсов в количестве, превышающем верхний пороговый уровень регистрации N_2. В результате переходная вероятность $P(0/1)$ уменьшается вплоть до наименьшего значения, а переходная вероятность $P(1/1)$ растет, достигая наибольшего значения. Таким образом, в диапазоне n_{s1}, на котором с увеличением n_{s1} переходная вероятность $P(1/1)$ растет, а переходная вероятность $P(0/1)$ уменьшается, наблюдается рост зависимостей $C_{\max}(n_{s1})$ и $D(n_{s1})$ за счет снижения отношения $P(0/1) / P(1/1)$ с увеличением n_{s1}. В диапазонах n_{s1}, на которых $P(1/1) \approx 1$ и $P(0/1) \approx 0$, зависимости $D(n_{s1})$ неизменны и близки к единице за счет того, что отношения $P(0/1) / P(1/1) \approx 0$, поэтому в этих диапазонах зависимости $C_{\max}(n_{s1})$ также практически неизменны и близки к единице (см. рисунок 1) [6].

Как видно из рисунка 1, в диапазонах средних скоростей счета сигнальных импульсов при передаче двоичных символов «1», на которых зависимости $C_{\max}(n_{s1})$ растут, увеличение средней длительности мертвого времени продлевающегося типа при прочих равных параметрах приема приводит к уменьшению пропускной способности канала связи. Так, например, при $n_{s1} = 33{,}5 \times 10^4$ с$^{-1}$ пропускная способность $C_{\max}$ равна 0,97 отн.ед. для $\tau_d = 0$; 0,87 отн.ед. для $\tau_d = 10$ мкс. Это объясняется тем, что в этих диапазонах значений n_{s1} увеличение τ_d при прочих равных параметрах приводит к снижению достоверности принятых данных. Такое снижение величины D обусловлено уменьшением переходных вероятностей $P(1/1)$ и ростом переходных вероятностей $P(0/1)$ с увеличением τ_d, что достаточно подробно исследовано в работе [6]. При увеличении τ_d максимумы статистических распределений $P_{st1}(N)$ сдвигаются в сторону меньших значений N. За счет этого смещения повышается вероятность регистрации на выходе счетчика фотонов импульсов в количестве, меньшем N_2, поэтому $P(1/1)$ уменьшается, а $P(0/1)$ растет. В результате имеет место рост отношения $P(0/1) / P(1/1)$, следовательно, уменьшаются достоверность принятых данных D [6] и пропускная способность канала связи $C_{\max}$.

Для исследуемого канала связи максимальная пропускная способность получена при наибольших значениях переходных вероятностей $P(0/0)$ и $P(1/1)$, которые с увеличением

τ_d, в свою очередь, обеспечиваются при более высоких значениях n_{s0} и n_{s1} соответственно: при $n_{s0} = 66{,}6 \times 10^3$ с$^{-1}$ и $n_{s1} \geq 35{,}0 \times 10^4$ с$^{-1}$ для $\tau_d = 0$; при $n_{s0} = 83{,}5 \times 10^3$ с$^{-1}$ и $n_{s1} \geq 43{,}7 \times \times 10^4$ с$^{-1}$ для $\tau_d = 10$ мкс.

Заключение

Применительно к асинхронному двоичному несимметричному однородному квантово-криптографическому каналу связи без памяти и со стиранием, содержащем в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа, установлены зависимости пропускной способности от средней скорости счета сигнальных импульсов при передаче двоичных символов «1».

Получено, что с ростом средней скорости счета сигнальных импульсов при передаче двоичных символов «1» пропускная способность канала связи увеличивается вплоть до насыщения, что наблюдается как при наличии мертвого времени продлевающегося типа, так и при его отсутствии. Причем при прочих равных параметрах приема увеличение средней длительности мертвого времени продлевающегося типа приводит к тому, что насыщение зависимостей $C_{\max}(n_{s1})$ наблюдается при более высоких значениях n_{s1}: при $n_{s1} \geq 35{,}0 \times 10^4$ с$^{-1}$ для $\tau_d = 0$; при $n_{s1} \geq 43{,}7 \times 10^4$ с$^{-1}$ для $\tau_d = 10$ мкс.

Результаты, полученные в настоящей работе, могут быть использованы при создании систем квантово-криптографической асинхронной связи, позволяющих с высокой достоверностью выявлять несанкционированный доступ к каналу связи за счет уменьшения погрешности определения количества ошибок легитимного приемного оборудования, в качестве которого используются счетчики фотонов с мертвым временем продлевающегося типа.

Список литературы

1. Щеглов, А.Ю. Анализ и проектирование защиты информационных систем. Контроль доступа к компьютерным ресурсам: методы, модели, технические решения / А.Ю. Щеглов. – СПб.: Профессиональная литература, 2017. – 416 с.
2. Килин, С.Я. Квантовая криптография: идеи и практика / С.Я. Килин; под ред. С.Я. Килин, Д.Б. Хорошко, А.П. Низовцев. – Минск: Белорус.наука, 2007. – 391 с.
3. Гулаков, И.Р. Фотоприемники квантовых систем: монография / И.Р. Гулаков, А.О. Зеневич. – Минск: УО ВГКС, 2012. – 276 с.
4. Тимофеев, А.М. Скорость передачи информации однофотонного канала связи с приемным модулем на основе счетчика фотонов с мертвым временем продлевающегося типа / А.М. Тимофеев // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. – 2019.– № 2. – С. 79–86.
5. Тимофеев, А.М. Методика повышения достоверности принятых данных счетчика фотонов на основе анализа скорости счета импульсов при передаче двоичных символов «0» / А.М. Тимофеев // Приборы и методы измерений. – 2019. – т. 10. – № 1. – С. 80–89.
6. Тимофеев, А.М. Достоверность принятой информации при ее регистрации в однофотонном канале связи при помощи счетчика фотонов / А.М. Тимофеев // Информатика. – 2019. – т. 16. – № 2. – С. 90–98.
7. Тимофеев, А.М. Устройство для передачи и приема двоичных данных по волоконно-оптическому каналу связи / А.М. Тимофеев // Приборы и методы измерений. – 2018. – т. 9.– № 1. – С. 17–27.

8. Тимофеев, А.М. Энтропия потерь однофотонного асинхронного волоконно-оптического канала связи с приемником на основе счетчика фотонов с продлевающимся мертвым временем / А.М. Тимофеев // Актуальные проблемы науки XXI века. – 2018. – вып. 7. – С. 5–10.

УДК 004.056

МЕТОДЫ ПОСТРОЕНИЯ КРИПТОСИСТЕМ БЕЗ КЛЕПТОМЕХАНИЗМОВ И ВЫЯВЛЕНИЯ КЛЕПТОГРАФИЧЕСКИХ МЕХАНИЗМОВ

А.И.ТРУБЕЙ, И.Б.БЕРЕЖНОЙ
Учреждение БГУ «НИИ прикладных проблем математики и информатики»
г. Минск, 220030, Республика Беларусь

Введение

Клептография (англ. Kleptography) – раздел криптовирологии, который исследует безопасные и скрытые коммуникации через криптосистемы и криптографические протоколы и асимметричные бэкдоры в криптографических алгоритмах (генерации ключей, цифровой подписи, обмене ключами, генераторах псевдослучайных чисел, алгоритмах шифрования) с целью совершения клептографической атаки. Еще в 1960-х ЦРУ, АНБ и немецкая БНД тайно получили контроль над всеми аспектами деятельности широко известной швейцарской фирмы Crypto AG, производившей шифраппаратуру в коммерческих целях: согласование набора персонала и клиентской базы, влияние на разработку аппаратно-программных средств, а также непосредственное вмешательство в устройства с использованием бэкдоров. Первейшей целью деятельности Crypto AG на протяжении десятилетий стала возможность ЦРУ читать переписку иностранных государств [1].

Действия спецслужб США затронули более 120 стран, в том числе Иран, Аргентину, Ватикан и Саудовскую Аравию. Как отметили в статье швейцарской медиакомпании SRF, «взломанные швейцарские устройства шифрования играли существенную роль, например, в рамках переговоров в Кэмп-Дэвиде в 1979 году, на переговорах об американских заложниках в Иране в 1981 году и во время американского вторжения в Панаму в 1989 году». Кроме того, декодированные телеграммы аргентинского военно-морского флота, передаваемые британцам немцами и американцами, внесли решающий вклад в победу Великобритании в войне 1982 года за Фолклендские острова.

К информационным потокам, которыми оперирует реализация одной из сторон криптосистемы, относятся источники случайности, канал приема данных от других сторон, каналы передачи данных другим сторонам, а также скрытые каналы утечек секрета, если рассматривать в контексте. клептографических модификаций. Для простоты будем считать, что есть только источник случайности (входной канал) и каналы передачи другим сторонам и разработчику (выходные каналы). Под такое упрощение подпадает, например, асимметричный криптопротокол на этапе генерации сессионной пары асимметричных ключей.

1. Мониторинг трафика и контроль целостности собственной реализации

К имеющимся сейчас методам обнаружением лазейки относятся мониторинг трафика и контроль целостности собственной реализации. Недостатками этих методов являются:

1.1 Мониторинг трафика не способен отследить SETUP (одно из требований к SETUP – невозможность наблюдателя отличить модификацию его от оригинала).

1.2 Контроль целостности затруднен тем, что в модели SETUP злоумышленник уже имеет доступ к реализации для модификации, следовательно, он также будет иметь возможность обойти контроль (например, перегенерировать подпись и заменить ключи проверки).

1.3 Если даже абонент имеет возможность контролировать целостность, он не способен проконтролировать целостность реализации своего оппонента.

Ключевым принципом работы системы с доказанной отсутствием клептографических лазеек является то, что ни один из абонентов системы не использует в протоколах внутренние источники случайности, а все псевдослучайные последовательности генерируются на базе публичных уникальных значений (счетчиков) с механизмами доказательства оригинальности (отсутствия модификаций). Это позволяет обеспечить выполнение достаточных условий об отсутствии канала незаметной утечки секрета.

2. Основные принципы создания криптосистемы с защитой от SETUP

К данным принципам относятся:

2.1 Каждый участник системы идентифицируется собственной парой асимметричных ключей.

2.2 Если конкретному участнику необходимо сгенерировать случайную последовательность, он генерирует ее исключительно на основе своего ключа- идентификатора и уникальных открытых значений (счетчиков), генерируемых оговоренным и одинаковым для всех способом (к примеру, простой инкремент.

2.3 В случае генерации такой последовательности, участник должен доказать другим сторонам протокола честность генерации.

То есть, в случае, когда протокол предусматривает использование источника случайности, участник может сгенерировать псевдослучайную последовательность на основе публичного счетчика, с использованием собственного секретного ключа, без использование собственных источников случайности, с невозможностью прогнозирования другими сторонами и возможностью доведения аутентичности данных. Для такой задачи могут быть применены схемы цифровой подписи без рандомизации, например, алгоритм цифровой подписи BLS, строящегося на конечных абелевых группах с определенными билинейными отображениями (например, криптографически стойкие эллиптические кривые с определенными функциями Вейля или Тейта, или алгоритм цифровой подписи RSA без рандомизации).

Подход к генерации псевдослучайной последовательности с публичного счетчика, кроме защиты от клептографических атак, имеет еще одно полезное свойство: он позволяет получить качественный генератор псевдослучайных последовательностей в случае отсутствия собственного источника случайности. Это актуально для виртуальных машин (доступ ко многим аппаратным ресурсам ограничен), систем IoT («интернета вещей»), систем на базе контроллеров без аппаратной поддержки источников случайности, толстых клиентов, когда большая часть логики веб ресурса переводится на мощности клиента, причем как правило средства обработки такой логики имеют ограниченный доступ к системным ресурсам.

3. Основные подходы к клептографическому анализу

Наряду с методами построения клептомеханизмов с доказанной отсутствием клептографических механизмов в криптосистемах важное значение также имеют методы выявления механизмов в существующих стандартах и реализациях.

Существует два принципиально разных подхода к клептографическому анализу:

3.1 Поиск собственного канала утечки через обнаружение модификаций реализации, использования классических методов криптоанализа примитивов и протоколов, анализ поведения абонентов и тому подобное. То есть считается, что криптосистема содержит клептографический механизм, если этот механизм фактически найден.

Преимущества первого подхода – подход является конструктивным, позволяет применить конкретные методы устранения канала утечки, возможна частичная автоматизация процесса обнаружения (например, контроль целостности при загрузке ПО, антивирусные средства и т.п.). Недостатками является наличие ошибки 2-го рода, то есть реально существующий клептомеханизм не обнаруживается в силу малой вычислительной мощности аналитика или ограниченности информации о потенциальной лазейке. Более того, если рассматривать устойчивость клептомеханизма к выявлению как задачу практической неразличимости, принципиально единственная возможность обнаружения – это переход к расширенной модели аналитика, что закладывается в дизайн лазейки. В случае высокого порога предусмотренных мощностей аналитика, это сделать практически невозможно.

3.2 Демонстрация отсутствия способов доказательства отсутствия канала утечки. То есть априори считается, что криптосистема содержит встроенный клептографический механизм, а задача анализа сводится к обоснованию невозможности такого построения. К данному методу, например, относится метод оценки клептографического потенциала, который не демонстрирует пути построения закладки, но показывает, что гипотетически такая возможность существует.

Преимуществами второго подхода является широкое покрытие алгоритмов с возможными каналами утечки и более простые (относительно первого подхода) методы оценки потенциальных каналов. Однако недостатками является наличие ошибки 1-го рода, что допускает наличие больших классов криптосистем, которые определяются как потенциально содержащие клептографические механизмы, хотя на самом деле они отсутствуют. Фактически, согласно этому подходу, криптосистемами без лазейки считаются только те, для которых формально доказано наличие достаточных условий отсутствия канала утечки секрета.

4. Базовая схема построения криптосистем без клептомеханизмов

Поскольку главной целью исследований является повышение уровня защищенности криптосистемы за счет уменьшения клептографических рисков, покажем место отдельных направлений клептографических исследований (клептоанализ, клептосинтез и построение криптосистем с доказанным отсутствием клептомеханизмов) в процессе повышения безопасности криптосистемы.

Построение криптосистем сегодня тесно связано с процессом разработки программных и программно-аппаратных комплексов, реализующих данные криптосистемы. Одной из проблем построения является то, что в связи с высокими темпами внедрений технических решений широко распространены «гибкие» подходы к разработке. Это значит, что на практике сложно внедрить строгий процесс контроля безопасности решений (в том числе и в клептографическом контексте) на каждом этапе жизненного цикла продукта. Фактически

программное проектирование, аудит защищенности продукта и осуществление мероприятий по уменьшению клептографических рисков являются параллельными и непрерывными процессами. В свою очередь, процесс повышения уровня информационной защищенности (в клептографическом контексте) также может состоять из параллельных процессов, что удобно укладывается в концепцию микросервисной архитектуры. На рисунке 1 приведен процесс уменьшения клептографических рисков криптосистемы.

В приведенном процессе (схеме) уменьшения клептографических рисков криптосистемы выходными артефактами является база известных клептографических механизмов, база известных криптографических примитивов и протоколов и собственно целевая криптосистема. Основа схемы – непрерывное взаимодействие параллельных процессов (блоков), каждый из которых отвечает за свою подзадачу.

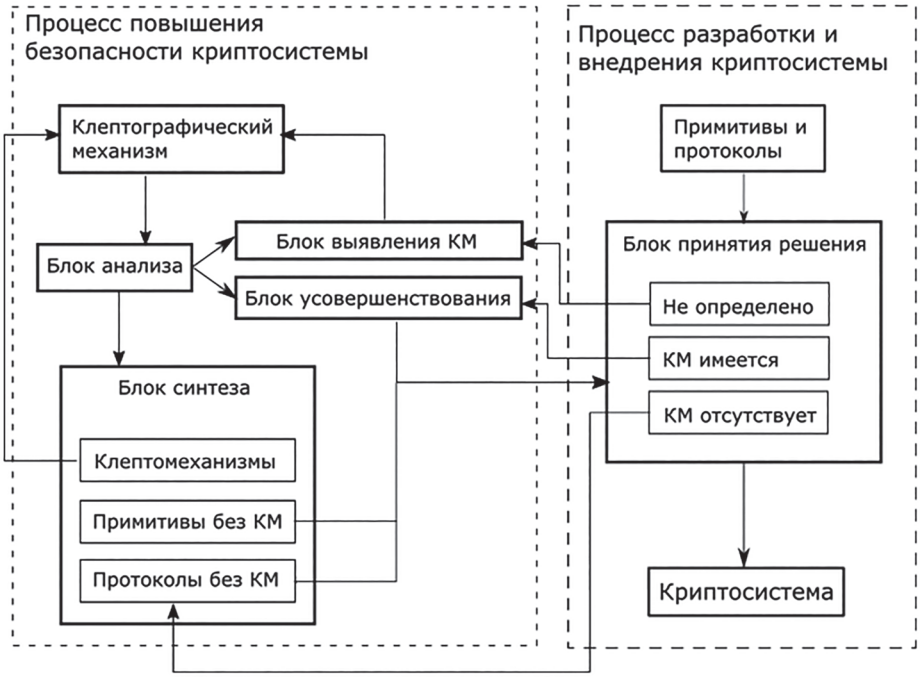


Рисунок 1. Процесс уменьшения клептографических рисков криптосистемы

4.1 Основные блоки в архитектуре схемы:

4.1.1 Блок анализа – анализ клептографических механизмов, классификация, построение формальной модели. На входе блока – известные клептографические механизмы, на выходе – формальная модель.

4.1.2 Блок синтеза – построение криптосистем с клептомеханизмами и с доказанным отсутствием закладок. Синтезированные клептомеханизмы используются для расширения пространства известных клептомеханизмов для дальнейшего анализа. На входе блока – формальные модели закладок и систем без них, на выходе – криптосистемы с закладками и криптосистемы с доказанным их отсутствием.

4.1.3 Блок обнаружения клептомеханизма – выявление клептомеханизма и клептоанализ, целью которого является расширение базы известных клептомеханизмов. На входе блока – криптосистема, определенная как содержащая закладку, на выходе – запись в базу клептомеханизмов.

4.1.4 Блок усовершенствования криптосистемы – модификация криптосистемы с закладкой или без так, чтобы модифицированная система была свободной от клептомеханизма. На входе блока – криптосистема, определенная как та, что содержит закладку, на выходе – модифицированная криптосистема без закладки.

4.1.5 Блок принятия решений – определяет содержит ли данная криптосистема лазейки. Блок принятия решений – это ключевой элемент клептографических взаимодействий мероприятий с реальным процессом разработки. Фактически здесь происходит принятие рисков, связанных с клептографическими атаками. Например, если блок определяет заданный криптопримитив как не содержащий лазейки, это означает только то, что в данном случае использование предполагается, что криптопримитив не содержит лазейки, а соответствующие риски приняты.

Приведенная схема является одним из простых возможных процессов улучшения функционирующей системы с относительно небольшими экономическими затратами, сравнительно с внедрением полного цикла разработки безопасного программного обеспечение, и может применяться ко многим практическим процессам разработки.

Заключение

В статье приведен обзор существующих методов выявления клептографических механизмов и их недостатков. Проведен анализ принципов создания криптографической системы с защитой от SETUP и существующих подходов к клептографическому анализу. Приведена базовая схема построения криптосистем без клептомеханизмов.

Список литературы

1. Endres F., Vögele N. Weltweite Spionage-Operation mit Schweizer Firma aufgedeckt. SRF, 2020 https:// www.srf.ch/news/schweiz/geheimdienstaffaere-cryptoleaks-weltweite-spionage-operation-mit-schweizer-firma-aufgedeckt.
2. Жуков, А., Маркелова, А. Криптография и клептография: скрытые каналы и лазейки в криптоалгоритмах / Information Security / Информационная безопасность – 2019 – № 1 – С. 36–41.
3. Шелест М.Е., Коваленко Б.А., Трубей А.И. Клептография vs криптография & стеганография // Теоретическая и прикладная криптография: Материалы международной научной конференции, Минск, 20–21 октября 2020 г. – С 106–113.
4. Simmons GJ. The Prisoners' Problem and the Subliminal Channel. в: Advances in Cryptology: Proceedings of Crypto 83. за ред. Chaum, D. Boston, MA: Springer US, 1984:51—67. doi: 10.1007/978-1-4684-4730-9_5. url: https://doi.org/10.1007/978-1-4684-4730-9_5.
5. Simmons GJ. The Subliminal Channel and Digital Signatures. в: Advances in Cryptology. за ред. Beth, T., Cot, N., Ingemarsson, I. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985:364—378.
6. 6. Kovalenko B., Kudin A., «Kleptography trapdoor free cryptographic protocols», Cryptology ePrint Archive, Report 2018/989, https://eprint.iacr.org/2018/989.
7. Young, A., Yung, M. The Dark Side of "Black-Box" Cryptography or: Should We Trust Capstone? в: Advances in Cryptology — CRYPTO '96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings. за ред. Koblitz, N. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996:89—103.
8. Bernstein, DJ., Chou, T., Chuengsatiansup, C та ін. How to Manipulate Curve Standards: A White Paper for the Black Hat Http://Bada55.Cr.Yp.To. в: Proceedings of the Second International Conference on Security Standardisation Research - Volume 9497. SSR 2015. Tokyo, Japan: SpringerVerlag, 2015:109—139. doi: 10.1007/978-3-319-27152-1_6. url: https: //doi.org/10.1007/978-3-319-27152-1_6.

004.056.53

МОДЕЛЬ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В. Б. ФИЛАТОВА
Университет ИТМО, Санкт-Петербург, 197101, Россия

В статье «Effectiveness of cybersecurity audit» авторы рассматривают взаимосвязь результативности аудита информационной безопасности с методом управления рисками. Авторы выдвигают гипотезу, что от результативности аудита кибербезопасности напрямую зависит уровень зрелости управления рисками, и обратно зависит возможность исполнения успешной кибератаки. В ходе исследования эта гипотеза была рассмотрена посредством интервью исследователей и главных аудиторов из разных стран и сфер деятельности. Было выяснено, что оценки Индекса аудита кибербезопасности находятся в большом диапазоне, где средним значением является 58 по шкале измерений от 0 до 100. Также, в статье определено, что несмотря на существующую прямую и тесную корреляцию этапов планирования и выполнения, эти этапы не имеют сильной зависимости с отчетами об эффективности управления рисками перед руководящим аппаратом предприятия, что может неблагоприятно отразиться на представлении реального состояния у управляющих.

В численном выражении планирование рассчитано с учетом ответов на девять вопросов о предупреждающих действиях внутреннего аудита и четырех вопросов о текущих действиях в области управления рисков.

Выполнение рассчитано через выражение процедур аудита, используемых для каждой из двенадцати областей рисков информационной безопасности в каждом цикле аудита и сумму четырнадцати инструментов, умноженную на вес показателя.

Гипотеза о том, что индекс аудита кибербезопасности тесно связан со зрелостью управления рисками, подтвердилась, но предположение о прямом влиянии этого индекса на реализацию атаки злоумышленника было опровергнуто.

Также, была рассмотрена статья «Методика оценки рисков на основе тестирования системы информационной безопасности» С. Е. Голикова. В ходе исследования Голиков описывает важность подобранной методики оценки рисков при дальнейшем тестировании состояния информационной безопасности. Автор обращается к рекомендациям по методу оценки рисков к таким источникам, как ГОСТ ИСО/МЭК 27005-2010, ГОСТ 13335-1 и NIST SP 800-30. Он приводит в пример модель управления рисками из NIST800-39, где представлен цикл таких процедур, как определение структуры, оценка, реагирование и мониторинг. Также автор затрагивает важность внедрения интегрированного подхода в области информационной безопасности, так как это позволяет рассматривать все элементы и процессы в качестве комплексной системы, где каждая составная часть влияет на другую.

По мнению автора, управление информационной безопасностью является процессом, входящим в более крупный процесс управления рисками - в исследовании сделан вывод о том, что если предприятие после изучения и оценки всех внутренних и внешних рисков делает вывод об актуальности рисков информационной безопасности, то, соответственно, появляется возможность свести к минимуму некоторые из них. В данной работе предлагается оценивать риски посредством выполнения тестирования на проникновение, а также

проведено сравнение некоторых подходов к тестированию для оценки рисков и последующему управлению ими.

Проведено сравнение разных методик оценки рисков и в статье «Review of cybersecurity assessment methods: Applicability perspective». Автор проводит регулярный анализ литературы и делает вывод, что исследования методов оценки рисков встречаются крайне редко. Автор ставит целью своей работы в рассмотрении с разных перспектив и последующем анализе методик оценки рисков информационной безопасности, которые определены в научной литературе. Для этого автор в своем исследовании использует подход структурированного наблюдения и выделяет тридцать два метода оценки процессов информационной безопасности на основе стандарта ИСО 31010, который содержит сорок два метода менеджмента рисков. Автор подчеркивает важность применимости методов в реальных условиях и ситуациях, и обозначает сложности и потенциальные проблемы, возникающие при использовании той или иной методики, а также вероятные способы избежать или решить их. В статье описаны отрасли, нуждающиеся в оптимизации и улучшении, а также дано направление для будущих исследований.

Была рассмотрена работа «Количественная оценка актуальности угроз информационной безопасности в проектируемых информационных системах», где автор предлагает метод количественной оценки актуальности угроз информационной безопасности в информационных системах на стадии их разработки. Для вычислений автор обращается к документу «Методика определения угроз безопасности информации в информационных системах», разработанному ФСТЭК России. В исследовании авторы выражают способы оценки рисков в количественной форме, основываясь на качественных определениях из таких нормативно-правовых источников, как ГОСТ Р ИСО/МЭК 27005-2010 и РС БР ИББС-2.2-2009. Автор учитывает термины и рассуждения из вышеперечисленных документов, задействуя такие факторы, как вероятность реализации угрозы, уровень проектной защиты и степень ущерба. В заключение автор предлагает использовать описанный метод для автоматизации расчетов при условиях возможности корректного численного выражения вышеназванных факторов.

В статье «Semi-quantitative cybersecurity risk assessment by blockade and defense level analysis» рассматривается оценка рисков информационной безопасности с точки зрения математики, статистики и информатики. Автор выдвигает мнение, что качественные академические модели оценки рисков не являются надежными для снижения вероятности киберугроз. В исследовании альтернативный способ оценки внутреннего риска путем проведения оценки риска предлагается в двух направлениях: определяется уровень риска источника возникновения угроз и оценивается уровень систем защиты, задействованных для устранения или карантина киберугроз, проникших внутрь.

Статья «Методика аудита и управления информационной безопасностью в государственном учреждении» раскрывает современные вопросы управления информационной безопасностью в государственном учреждении. Автор описывает, как аудит системы управления информационной безопасностью, так и локальные вопросы управления рисками. В исследовании определено, что на результативное и комплексное управленческое решение в системе управления информационной безопасностью влияет выполнение процедур, способствующих сведению рисков к минимуму в данной системы. Процесс принятия решения основан на классических принципах с использованием системного и математического подходов. Авторы обосновывают методику аудита и управления информационной безопасностью с применением принципов системного анализа, swot-анализа, методов структури-

зации, экспертного опроса и статистической обработки результатов экспертного опроса. Система управления информационной безопасностью в предложенной методике рассматривается как комплекс факторов - законодательного, административного, технического, организационного и социально-психологического.

В ходе анализа вышеизложенной литературы сделано заключение, что количественная оценка риска является наиболее предпочтительным подходом в риск-менеджменте.

Как правило, оценка рисков базируется на двух аспектах: вероятность возникновения угрозы и серьезность возможных последствий. Из этого следует классификация, полученная из матрицы: в ней риски определяются по шкале от низкого до критичного. Среди основных минусов такого подхода можно выделить:

- невозможность точно идентифицировать некоторые риски, занимающие пограничное положение в процессах организации
- Сложность переоценки риска при изменении среды и влиянии новых условий
- Оценка носит более теоретический характер, нежели объективный

Для создания модели необходимо выделить факторы, связанные с рисками, а также потенциальными последствиями, а после определить их взаимосвязь и выразить ее в количественной форме. Относительно вероятности возникновения угрозы существует следующие влияющие моменты:

1. Частота возникновения угрозы в прошлом
2. Процентное соотношение причин возникновения: человеческий фактор и произвольный Касаемо серьезности потенциальных последствий:
   1) Доля материального ущерба от средней прибыли за выбранный период
   2) Степень репутационного ущерба
   3) Издержки на восстановление
   4) Срок устранения последствий
   5) Взаимосвязь угрозы с другими компонентами системы

Из перечисленных составных частей риска не все можно свести к точному числу: например, потенциальный репутационных ущерб подсчитать не представляется возможным, и этому фактору можно присвоить коэффициенты в соответсвии с качественной шкалой.

После того, как эти факторы будут посчитаны по построенной формуле, необходимо отнести результат этих вычислений к распределению, какое значение означает критичный риск, а какое незначительный. Для этого предлагается оценивать степень тяжести риска по воздействию на производственный процесс, например:

1. Полная остановка производства - критичный;
2. Нарушение плана производства двух и более компонентов предприятия, финансовые потери превышающие прибыль - высокий;
3. Нарушение плана производства одного компонента предприятия - средний;
4. Событие, практически не повлиявшее на производство - низкий.

Для достоверного числового распределения необходимо установить, какая угроза или совокупность угроз приведет к тому или иному последствию.

Выводы.

Полностью отказаться от использования принципа качественной классификации в управлении рисками и действовать только расчетным, методом, к сожалению, невозможно. Но повысить точность модели оценки, и как следствие, предотвратить неблагоприятные

последствия или устранить их с меньшими издержками можно при использовании вышеописанных формул.

Список литературы

1. https://www.sciencedirect.com/science/article/pii/S1467089521000506
2. https://www.researchgate.net/publication/323759002_Empirical_study_on_the_integrated_management_system_in_Algerian_companies
3. https://www.elibrary.ru/item.asp?id=47154847
4. https://www.sciencedirect.com/science/article/pii/S0167404821002005
5. https://www.elibrary.ru/item.asp?id=32346373
6. https://www.sciencedirect.com/science/article/pii/S0957582021004948
7. https://www.elibrary.ru/item.asp?id=43099110

УДК 621.391.82

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ КАНАЛОВ УТЕЧКИ ВИДЕО ИНФОРМАЦИИ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ

С.В.ХАРЧЕНКО, В.К.ЖЕЛЕЗНЯК
УО «Полоцкий государственный университет»
г. Новополоцк, 211440, Республика Беларусь

1. Введение

Необходимость написания данной статьи обусловлена отсутствием исследований информационных полей и особенностей каналов утечки видео информации ПК. Полученные в ходе исследования и описанные в статье результаты будут являться частью разрабатываемой методики оценки защищенности видео информации ПК.

Цель: исследовать и показать особенности каналов утечки видео информации ПК, влияющие на оценку защищенности.

Защита информации (ЗИ) – научно обоснованные технические, аппаратно-программные, программные, криптографические и другие методы и средства, организационные, юридические меры, реализующие защищенность. Защищенность – способность информационной системы противостоять утечке информации по техническим каналам, несанкционированному доступу к программам, информации, умышленному или случайному их искажению или разрушению [1].

Предметом защиты информации являются источники информационных физических полей рассеивания, процессы излучения этих полей, их распространения, наводок, локализации, маскирования и извлечения, модели каналов утечки информации (КУИ), методы, алгоритмы, средства оценки (измерения) параметров и характеристик каналов утечки информации, меры защиты информации, информационные параметры и параметры селекций, а также характеристики маскирующих шумов [1].

В качестве объекта исследования выступает ПК с внешним видеомонитором. Основным каналом утечки видео информации является паразитные электромагнитные излучения

и наводки (ПЭМИН). Сложность данного канала утечки информации заключается в том, что при передаче информации на видеомонитор по средствам кабелей, возникают электромагнитные излучения, которые при попадании на проводник (антенну считывающего устройства), порождают в нем ток, схожий с оригиналом. После дискретизации считанного сигнала можно восстановить данные передаваемые через проводник, что может привести к утечке информации. Однако сигнал может не только напрямую излучаться от различных проводников, по которым непосредственно передается информация, электромагнитные излучения могут спокойно ретранслироваться через различные электропроводимые материалы.

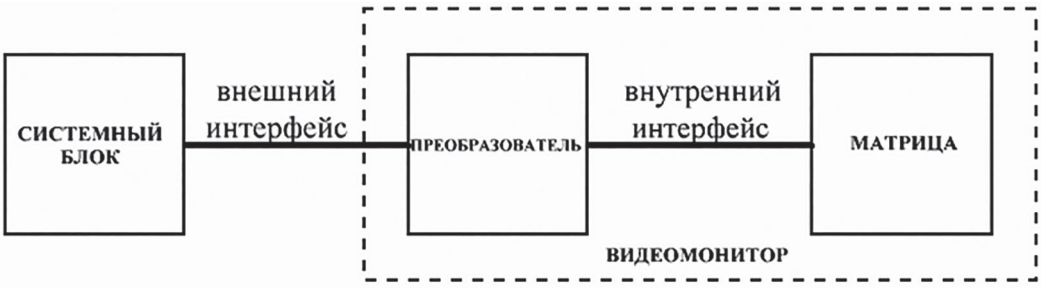


Рисунок 1. Блок схема ПК

Основными источниками ПЭМИ в исследуемом ПК являются следующие интерфейсы передачи видео информации:

- Digital Visual Interface, сокр. DVI (с англ. — «цифровой видеоинтерфейс») — стандарт на интерфейс, предназначенный для передачи видеоизображения на цифровые устройства отображения, такие как жидкокристаллические мониторы, телевизоры и проекторы. В исследуемом ПК является внешним интерфейсом.
- Low-voltage differential signaling, сокр. LVDS (с англ. низковольтная дифференциальная передача сигналов) — способ передачи электрических сигналов и стандарт ANSI/TIA/EIA-644-A 2001 года, позволяющий передавать информацию на высоких частотах при помощи дешёвых соединений на основе медной витой пары. В исследуемом ПК является внешним интерфейсом.

В исследуемом ПК интерфейс DVI служит для передачи видео информации от видео адаптера 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 интерфейса LVDS видео информация от видеоконтроллера видеомонитора передаётся на плату драйверов матрицы.

2. 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 и последующей обработки полученных данных удалось построить спектрограммы в частотных диапазонах 50 МГц – 1000МГц, и 1000 МГц – 10 000 МГц соответственно:

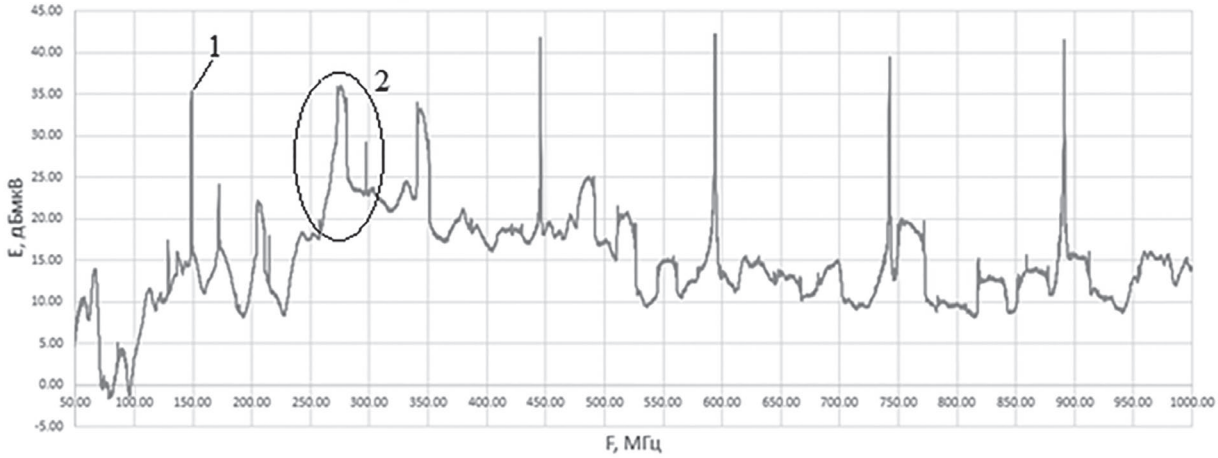


Рисунок 2

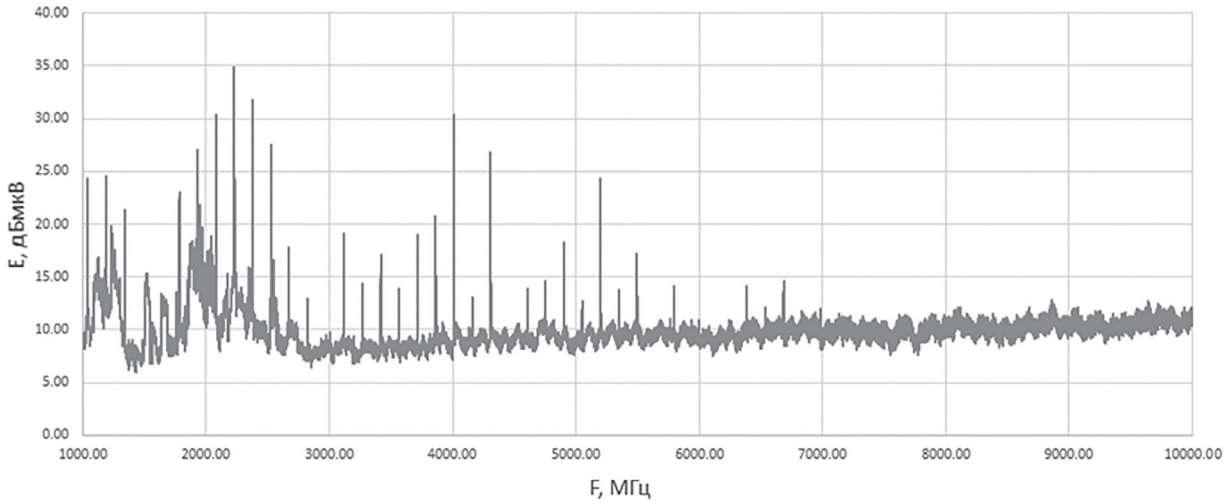


Рисунок 3

На полученных диаграммах отчетливо выделяются два сигнала:

- узкополосный сигнал с частотой повторения $F_{т1}$=149 МГц и его гармонические составляющие;
- широкополосный сигнал с частотой повторения $F_{т2}$=34.65 МГц и его гармонические составляющие.

В результате различных манипуляций с испытуемым ПК (изменение видео сигнала, отключением питания видео контроллера, отсоединения кабеля интерфейса DVI и др.), удалось установить, что узкополосным сигналом является информационный сигнал, передаваемый по интерфейсу DVI, в свою очередь широкополосным сигналом является информационный сигнал, передаваемый по интерфейсу LVDS. Источником информационного сигнала является видео адаптер ПК, следовательно, узкополосный и широкополосный сигналы несут одну и ту же информацию, преобразованную по различным протоколам. Исходя из этого, в плане ЗИ необходимо рассматривать интерфейсы DVI и LVDS по отдельности.

3. Особенности КУИ интерфейса DVI

3.1. Использует технологию высокоскоростной передачи цифровых потоков TMDS (Transition Minimized Differential Signaling — дифференциальная передача сигналов с минимизацией перепадов уровней) — три канала, передающие потоки видео и дополнительных данных, с пропускной способностью до 3,4 Гбит/с на канал.

3.2. Частотный диапазон излучения информационных сигналов.

Информационные излучения интерфейса DVI ограничены частотным диапазоном 30 МГц – 10 ГГц.

4. Особенности КУИ интерфейса LVDS

4.1. Стандарт ANSI/TIA/EIA-644-A.

4.2. Частотный диапазон излучения информационных сигналов.

Информационные излучения интерфейса LVDS ограничены частотным диапазоном 30 МГц – 5 ГГц. Изучение информационных излучений в широком диапазоне частот требует наличие высокоточной измерительно аппаратуры специального экранированного помещения для измерений.

4.3. Функция «размазывания спектра».

Одной из особенностей интерфейса LVDS является программное включение функции «размазывания спектра». Функция заключается в том, что вся информации заключается не в одной гармонике в виде узкополосного сигнала, а «размазывается» в широкополосный сигнал. Спектрограммы измерения излучения интерфейса LVDS при выключенной функции «размазывания спектра» рисунок 4, и при включенной функции рисунок 5:

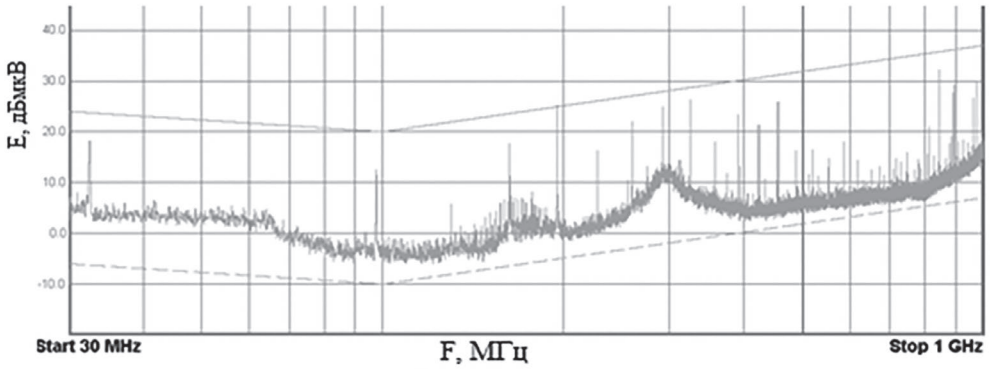


Рисунок 4

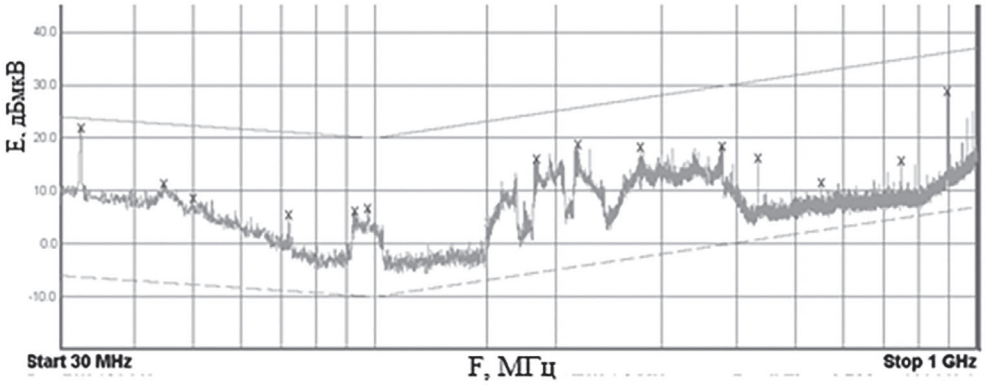


Рисунок 5

Данная функция позволяет маскировать информационные излучения в шумах, но усложняет проведение исследования информационных излучений.

5. Выводы:

В результате исследования удалось выявить и показать особенности каналов утечки видео информации ПК. При разработке методики оценки защищенности ПК необходимо учитывать следующие особенности:

- Исследуемые интерфейсы передачи видео информации используют разные стандарты кодирования информации для её последующей передачи. Из этого следует, что создания методики оценки защищенности видео информации необходимо разрабатывать информационные тестовые сигналы для каждого интерфейса отдельно.
- Крайняя граница диапазона частот для исследования каналов утечки видео информации при рассмотрении интерфейсов DVI должна быть не ниже – 10 ГГц.
- Крайняя граница диапазона частот для исследования каналов утечки видео информации при рассмотрении интерфейсов LVDS должна быть не ниже – 5 ГГц.
- При исследовании широкополосных информационных сигналов необходимо рассматривать сигнал как интеграл площади по частоте.

Список литературы

1. Железняк В. К. Защита информации от утечки по техническим каналам: учебное
2. пособие. – ГУАП. – СПб. 2006. – 188 с.
3. Князев, А.Д. Конструирование радиоэлектронной и электронно-вычислительной аппаратуры с учётом электромагнитной совместимости // А. Д. Князев, Л. Н., Кечиев, Б.В. Петров. – М.: Радио и связь, 1989. – 224 с. ил.
4. Бузов Г. А. Защита от утечки информации по техническим каналам: Учебное пособие / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. – М.: Горячая линия – Телеком, 2005. – 416 с.: ил.
5. Уайт Д. Электромагнитная совместимость и непреднамеренные помехи. В 3-х выпусках. — Москва: Советское радио, 1977. — 352 с.
6. Князев А.Д. Элементы теории и практики обеспечения электромагнитной совместимости радиоэлектронных средств / А. Д. Князев. - Москва: Радио и связь, 1984. - 336 с. : ил.

УДК [004.42:373]: 004.056.5

ЗАЩИТА МОБИЛЬНЫХ УСТРОЙСТВ СОТРУДНИКОВ ПРЕДПРИЯТИЙ И ШКОЛЬНИКОВ – ОДНА ИЗ ОСНОВ УСПЕШНОЙ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ И СОЦИАЛЬНОЙ СФЕРЫ БЕЛАРУСИ

И.И. ШПАК, В.Д. АЛЕНИН, Н.И. БАХУР
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»,
г. Минск, Республика Беларусь

Введение

Цифровизация экономики и всех сфер жизнедеятельности белорусского общества, в соответствии с Государственной программой [1], предусматривает не только внедрение информационно-коммуникационных технологий (ИКТ) и передовых производственных технологий во все отрасли народного хозяйства и социальную сферу, но также требует обеспечения защиты информации.

Решение задач по защите информации выполняется путем реализации мероприятий в рамках отдельной подпрограммы: “Информационная безопасность и “цифровое доверие”. Реализация указанной подпрограммы должна обеспечить повышение уровня информационной безопасности во всех сферах человеческой деятельности, защиты прав и законных интересов граждан [1].

Одной из важнейших задач по обеспечению защиты информации является разработка организационных и программных способов защиты мобильных устройств сотрудников предприятия на рабочих местах от вредоносного программного обеспечения (ВПО), от хищения персональных данных, а также от хищения служебного контента [2]. Аналогичные способы можно использовать для защиты мобильных телефонов школьников во время занятий в «Электронной школе» [3]. Весьма перспективной для указанных целей является технология *Byod (Bring your own device)* [4].

1. Анализ, достоинства и ограничения технологии *BYOD* «Принеси свое собственное устройство»

В 2004 году Рафаэль Баллагос *(Rafael Ballagas)* с соавторами опубликовал статью «*Byod: Bring your own device*» [4], в которой предложил подход к организации учебного процесса на предприятии с большими публичными дисплеями. *BYOD* на русский язык переводится как «Принеси свое собственное устройство». В настоящее время синонимами слова «подход *BYOD*» стали термины технология, стратегия, концепция, политика.

При применении *BYOD* обучаемый использовал принадлежащее ему устройство для доступа к информационным ресурсам учебного заведения или предприятия. При этом в статье [4] под устройством понимался мобильный телефон Nokia 6600 с камерой. *BYOD* по Баллагосу не только вносил в обучение эффект новизны и привлекал внимание обучаемого, но и позволял ученикам работать онлайн с электронными методическими пособиями, наглядными материалами и проверочными заданиями. Такой подход экономил время: больше не нужно было искать страницу в учебнике, перерисовать график или выписывать термины в тетрадь, а результаты теста можно было узнать сразу после прохождения [4]. Так, на конференциях *Digital Learning*, посвященных развитию цифровых технологий в обучении, провозглашался лозунг: «Зарегистрируйтесь по промокоду mobile2019 — и создавайте собственные курсы» [4]

В последующие годы использование технологии *BYOD* как концепции использования личных персональных гаджетов (смартфонов, планшетов, ноутбуков, жестких дисков или USB-накопителей, коммуникаторов (гибридов мобильного телефона и карманного компьютера, снабженных рядом программ) и т д.) сотрудников в рабочих целях стало повсеместным за счет ускорения бизнес-процессов: *BYOD* позволяет в рабочее время практически мгновенно получать актуальную информацию и упрощает коммуникацию сотрудника с коллегами. Мобильные технологии существенно изменили подходы к обучению. Сам процесс обучения стал более комфортным и быстрым. Организация Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО), совместно с Институтом ЮНЕСКО

по информационным технологиям в образовании (ИИТО ЮНЕСКО), ввела специальный термин «мобильное обучение» и разработала рекомендации по его широкому внедрению [5]

Концепция *BYOD* достигла популярности после ее внедрения компанией «*Intel Corp.*» (США, Пенсильвания), крупнейшим в мире разработчиком и производителем электронных устройств и компьютерных компонентов (микропроцессоров и др.). По данным *Intel* количество мобильных устройств, используемых на работе служащими Intel, в 2009-2010 годах выросло с 10 до 30 тысяч. Предполагалось, что к 2014 году примерно 70% работников *Intel* будут использовать на работе собственные личные устройства [6].

Усилиями компьютерных фирм США «*Unisys Corp.*» (Пенсильвания), «*VMware Co.*» (Калифорния) и «Citrix Systems, Inc.» (Флорида) стратегия *BYOD* получила новый импульс к развитию, и ее техническая реализация оказалась вполне доступной [7]. *BYOD* стали использовать известные международные корпорации со штаб-квартирами в США «*Cisco Systems Inc.*» (Калифорния), «IBM *Corp.*» (штат Нью-Йорк), «*Oracle Corp.*» (Техас), а также канадская «*BlackBerry Ltd.*» (организационно-правовые формы компаний США (Co, *Corp. LP, Inc., Ltd.* и др.) кратко рассмотрены в [8].

Достоинствами *BYOD* являются [6]:

- Экономия бюджета. *BYOD* также может положительно сказаться на расходах работодателей, поскольку они не оплачивают покупку устройства заранее или не тратят средства на расходы по обслуживанию/обновление в будущем;
- Эффективность. Сотрудникам легче, быстрее и комфортнее выполнять рабочие обязанности с того устройства, которое им знакомо и привычно. В свою очередь это повышает производительность труда и максимизирует прибыль от бизнеса.
- Лояльность. Позволяя использовать личное оборудование в работе, компания повышает уровень доверительных отношений с сотрудниками.

Таким образом, если работники предприятия почти не расстаются со смартфонами, они начинают и заканчивают свой день, проверяя рабочую почту, и находятся в постоянном доступе [7].

Однако при перечисленных преимуществах, у *BYOD* имеются и недостатки, сводящие на «нет» достоинства преимуществ:

Опасность заражения личного смартфона сотрудника вирусами и шпионскими программами. Вирус препятствует работе сотрудника. При заражении им сотрудник утрачивает возможность использовать смартфон, что снижает производительность труда сотрудника.

Шпионская программа позволяет злоумышленнику считать с зараженного смартфона служебную информацию, которой сотрудник пользуется во время работы. Этот объем конфиденциальной информации и информации, составляющей коммерческую тайну, может интересовать конкурентов предприятия, а ее утечка непосредственно влияет на производственную безопасность предприятия.

Опасность кражи и утери личного смартфона. Устройство сотрудника может быть украдено или утеряно вместе со всей служебной информацией.

Для устранения этих недостатков существует практика административного запрета сотрудникам во время работы использовать личные смартфоны. Вместо личных устройств сотрудника, ему в часы его работы выдается служебный смартфон предприятия, контролируемый службой информационной безопасности (СИБ).

2. Результаты проведенных работ по защите мобильных устройств сотрудников предприятий и школьников в Беларуси

Решение поставленной задачи целесообразно начать с рассмотрения существующих в рамках технологии *BYOD* моделей, сложившихся к настоящему времени. В интернет-ресурсе 2021 года [9] перечислены следующие модели *BYOD* и их аббревиатуры, отражающие весь спектр устройств:

- *BYOT – Bring Your Own Technology* - Принеси свою собственную технологию*;*
- *BYOP – Bring Your Own Phone* - Принеси свой собственный телефон*;*
- *BYOPC – Bring Your Own Personal Computer* - Принеси свой собственный персональный компьютер.
- *BYOM – Bring Your Own Meeting* – Организуй свою собственную встречу (коммуникатор)*;*
- используемых в рамках концепции *BYOD* и решаемых с ее помощью задач. Применительно к *BYOP* это могут быть две подмодели:
- *POCE (Personally-Owned, Company Enabled)* – смартфон в личной собственности сотрудника, но с поддержкой компании. Эта модель похожа на *BYOD*, при этом компания берет на себя ответственность за часть возможностей устройства, используемых в бизнес-целях. Доступ к корпоративной сети осуществляется через портал, программно отделенный от частной части устройства.
- *COBO (Corporate-Owned, Business-Only)* – сотрудник получает служебный смартфон, который используется только для бизнеса. Эта модель наиболее востребована специалистами СИБ.

В подмодели *COBO* смартфон проще и эффективнее защищать, используя общепринятые мировые практики защиты *BYOD* [9]. В служебных смартфонах доля смешивания личных и профессиональных данных мала, поэтому некоторые ограничения свободы действий пользователя оправданы и целесообразны. В этом случае баланс смещен более в сторону защиты данных, нежели удобства использования. Для этих целей можно использовать как специализированные устройства *(Blackberry)*, так и специальные превентивные меры по предотвращению утечек.

Одной из таких мер является внедрение *MDM (Mobile Device Management)* – (Управление мобильными устройствами). Системы класса *MDM* позволяют СИБ удаленно (централизованно) управлять множеством мобильных устройств (в т. ч. и смартфонов), будь то устройства, предоставленные сотрудникам компанией, или собственные устройства сотрудников.

Управление мобильными устройствами обычно включает в себя такие функции, как удаленное обновление политик безопасности (без подключения к корпоративной сети), распространение приложений и данных, а также управление конфигурацией для обеспечения всех устройств необходимыми ресурсами.

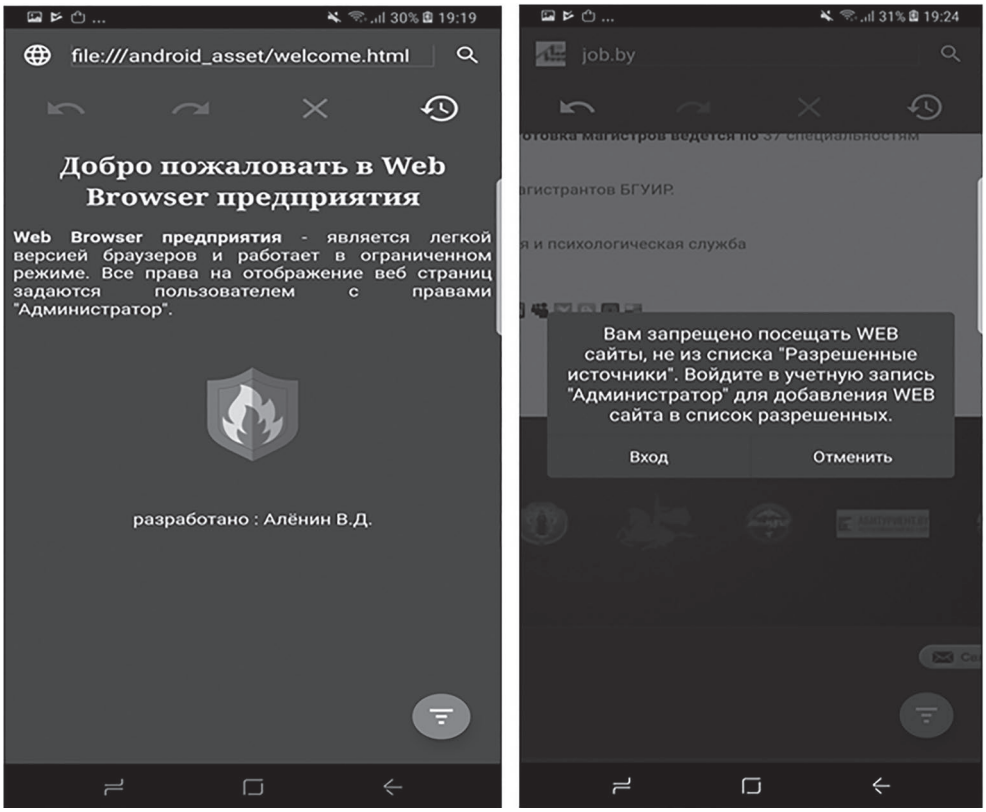
MDM-решения составляют основную часть программного обеспечения (ПО), активно продаваемого на рынке ПО *BYOD*. По данным *Global Industry Analysts, Inc*, в 2022 году объем рынка *BYOD* достигнет почти $94,2 млрд. Для сравнения, в 2014 году это значение составляло $30 млрд [10].

Внедрение *BYOD/COBO* на белорусских предприятиях, на наш взгляд, невелико, так как в Беларуси нет предприятий в сфере телекоммуникаций и информатики, сравнимых по чистому годовому доходу (прибыли, ЧД) с вышеупомянутыми *Oracle* (ЧД $13,7 млрд), *Cisco* (ЧД $10,6 млрд), *IBM* (ЧД $5,59 млрд) или даже *Citrix* (ЧД $536 млн).

Самое крупное белорусское предприятие Белтелеком получило в 2020 году чистую прибыль всего $83 млн. Поэтому предприятия Беларуси практически не защищают свои корпоративные ЛВС путём покупки за рубежом дорогостоящих *MDM*-решений.

Таким образом, в Беларуси на рабочем месте белорусского сотрудника не то что предпочтительнее, а в силу недостатка денег, до сих пор используется личный смартфон (чистый *BYOD* по Баллагосу или изредка *BYOD/ POCE* с *MDM*-решениями белорусских программистов.

Однако после введения санкций, запрещающих передачу России и Беларуси передовых информационных технологий, рынок *MDM* и *BYOD* для Беларуси вообще стал закрытым. В этих условиях в Институте информационных технологий Белорусского государственного университета информатики и радиоэлектроники (ИИТ БГУИР) разработано простое *MDM*-решение «Б» для установки на смартфонах с мобильной операционной системой *Android* [11]. Экранные формы приложения «Б» приведены на рисунке 1.



а) б)

Рисунок. Экранные формы приложения «Б»

Приложение «Б» реализовано на языке программирования *Java* и имеет объём 27Mb. Смартфоны с *Android* были выбраны потому, что в соответствии с годовым отчётом *CISCO* по информационной безопасности за 2014 год 99 % мобильного вредоносного ПО было нацелено на устройства под управлением *Android* [12]. Приложение «Б» может устанавливаться как на личный смартфон, работающий по технологии *BYOD*, модель *BYOP*, подмодель *POCE*, так и на служебный смартфон (подмодель *COBO*). В свое время приложение «Б» прошло апробацию на личных смартфонах школьников в проекте «Электронная школа»

(руководитель апробации от ИИТ БГУИР – Н.И. Бахур [3].). Приложение «Б» при использовании подмодели *COBO* блокирует доступ пользователя смартфона ко всем веб-ориентированным приложениям кроме тех, которые разрешены для использования администратором сети или СИБ предприятия, с целью выполнения пользователем своих служебных обязанностей. В число заблокированных попадают адреса вредоносных сайтов, содержащих вирусы или шпионские программы, а также адреса игровых сайтов (на работе трудись, а не играй!). Для подмодели *POCE* блокируются только адреса вредоносных сайтов.

На рисунке 1 а) показана экранная форма приложения «Б» для задания адреса разрешённого сайта, а на рисунке 1 б) – форма, которую видит владелец смартфона при попытке посетить заблокированный неразрешённый сайт [11].

Заключение

1. Рассмотрены технологии и модели, используемые для защиты мобильных устройств сотрудников предприятий и школьников в Беларуси.
2. Проведен анализ возможностей и состояние внедрения *BYOD* на белорусских предприятиях и в школах.
3. Для безопасности личных смартфонов по модели «чистый *BYOD* по Баллагосу» или *BYOD/ POCE* предложено *MDM*-решение собственной разработки, защищающее смартфоны с операционной системой *Android*.

Список литературы

1. Государственная программа «Цифровое развитие Беларуси» на 2021 – 2025 годы. [Электронный ресурс]. – Режим доступа: https://mpt.gov.by/ru/gosudarstvennaya-programma-cifrovoe-razvitie-belarusi-na-2021-2025-gody /⁉ – Дата доступа 22.04.2022.
2. Алёнин, В.Д. Угрозы информационной безопасности при использовании мобильных устройств на рабочих местах и в школах и их парирование / В.Д. Алёнин и др./ - Информационные системы и технологии ИСТ-2017, 2017 С. 569-573.
3. Бахур, Н. И. Модели и средства обеспечения управления информационной безопасностью на примере проекта «Цифровая школа»: автореф. дисс. на соискание степени магистра технических наук: 1-98 80 01 / Н. И. Бахур; науч. рук. И. И. Шпак. - Минск : БГУИР, 2016. - 10 с.
4. Мобильное обучение. [Электронный ресурс]. – Режим доступа: https://we.study/blog/mobile/⁉ – Дата доступа 22.04.2022.
5. Рекомендации по политике в области мобильного обучения. [Электронный ресурс]. – Режим доступа: https://iite.unesco.org/pics/publications/ru/files/3214738.pdf /⁉ – Дата доступа 22.04.2022.
6. Что такое *BYOD*? [Электронный ресурс]. – Режим доступа: https://unitsolutions.ru/blog/terminologiya/chto-takoe-byod /⁉ – Дата доступа 22.04.2022.
7. Темная сторона *BYOD*. [Электронный ресурс]. – Режим доступа: https://ko.com.ua/temnaya_storona_byo_99426 /⁉ – Дата доступа 22.04.2022.
8. Николаенко В.Л., Сечко Г.В., Таболич Т.Г. Технологии радиочастотной идентификации на автомобильном транспорте. Современное состояние и история развития по патентам США. Гродно: ЮрСаПринт, 2021. 238 с.
9. *BYOD* — Удобство против безопасности. [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/281463/. – Дата доступа 22.04.2022.
10. 10. Что такое *BYOD*? Модели *BYOD*. [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/ipmatika/blog/584014/. – Дата доступа 22.04.2022.

11. Алёнин, В.Д. Информационная безопасность мобильных систем *Android*: диссертация на соискание степени магистра технических наук: 1-98 80 01 / В.Д. Алёнин; науч. рук. И. И. Шпак. - Минск : БГУИР, 2017. - 63 с.
12. Хуг, Эндрю. Мобильная безопасность: битва вокруг вредоносного ПО // Безопасность ИТ-инфраструктуры. 2014. N 7 (85). С. 4–6.

СОДЕРЖАНИЕ

ПРИКЛАДНЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ КРИПТОГРАФИЧЕСКОЙ И ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

АКТУАЛЬНЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЮЗНОГО ГОСУДАРСТВА

ВВОПРОСЫ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

ПОДГОТОВКА КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЗАОЧНЫЕ ДОКЛАДЫ

Научное издание

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ
Материалы XXVII научно-практической конференции,
24–26 мая 2022 г.

Подписано в печать 14.06.2022. Формат 60×84 1/8.
Бумага офсетная.

Тираж 60 экземпляров.
ООО «Медиа Группа «Авангард»
Россия, Москва, 127473, 3-й Самотечный пер., д. 21
www.avangardpro.ru