Структурное содержание требований информационной безопасности

Марков А. С., Цирлов В. Л. [1]

Ключевые слова: *кибербезопасность, информационная безопасность, техническая защита информации, тенденции, тренды, прогнозы, общие критерии, ИСО 15408, механизмы безопасности, организационно-технические меры, правовые основы, руководящие документы, стандарты.*

Аннотация. *Рассмотрены основные события в области информационной и кибербезопасности за последние несколько лет. Выявлены новые феномены информатизации общества, связанные с областью информационной безопасности. Выделены основные тенденции в различных сегментах информационной безопасности. Проведен краткий обзор доктрин безопасности, законодательной основы отрасли информационной безопасности. Показаны инновационные направления деятельности регуляторов отрасли, кающиеся применения риск-ориентированного подхода, комплекса организационно-технических мер, международного подхода по оценке соответствия ИТ-изделий требованиям по безопасности информации, повышению результативности проверок по информационной безопасности. Отмечены преимущества и проблемные моменты применения указанных подходов. Показаны имеющиеся неопределенности в подходах, снижающие уровень унификации в области технической защиты информации. Даны предложения по совершенствованию нормативно-правового обеспечения информационной безопасности.*

DOI: 10.21681/2412-8163-2017-1-53-61

1. Введение в проблематику

Востребованность анализа нормативно-правового применения [1, с.5] в области обеспечения информационной безопасности (ИБ) можно связать с двумя феноменами информатизации общества, появившимися за последние три года:

– предсказания в области компьютерных инцидентов и событий в области информационной безопасности сбываются, т.е. специалисты понимают проблематику ИБ;

– продолжается нарастание политического противостояния государств в киберпространстве.

Первое утверждение легко проверить, сравнив не только ежегодные объективные отчеты и бюллетени по информационной безопасности известных ИТ-корпораций, как-то: AT&T, Cisco, Dell, Google, IBM (X-Force), Kaspersky, McAfee, Sophos, Symantec, Verizon, но и проанализировав ресурсы блогосферы. Например, прогнозы популярного эксперта-блоггера по событиям ИБ в России на 2016 год сбылись более чем на 80%[2]. Указанное позволяет сделать вывод, что концептуальные подходы к оценке и планированию отрасли ИБ понятны, и вопрос состоит лишь в реализации их на практике с учетом меняющихся конкретных условий.

Можно отметить наиболее актуальные проблемные темы ИБ на текущий год:

– сложность обнаружения целенаправленных вредоносных атак (APT-атак);

– безопасность Интернет-вещей;

– рост требований по защищенности тайны частной жизни;

– проблема больших данных;

– доступность инструментария хакеров;

– высокий уровень уязвимости прикладных систем.

Второе утверждение связано с уникальными возможностями киберпространства для реализации «мягкой силы» в информационном противоборстве. Как известно, кибервойны характеризуются такими свойствами, как анонимность (без-

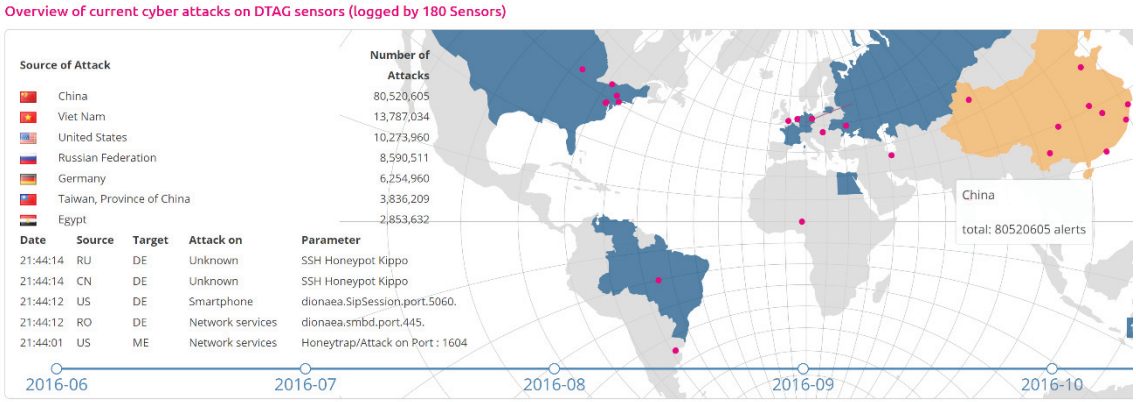
[2] http://lukatsky.blogspot.ru/2016/12/blog-post_27.html

[1] ***Марков Алексей Сергеевич,*** *доктор технических наук, старший научный сотрудник, профессор МГТУ им.Н.Э.Баумана, Российская Федерация, г. Москва.*

E-mail: *a.markov@bmstu.ru*

Цирлов Валентин Леонидович, *кандидат технических наук, генеральный директор ЗАО «НПО «Эшелон», Российская Федерация, г. Москва.*

E-mail: *z@cnpo.ru*



Источник: sicherheitstacho.eu (10.01.2017)

Рис. 1. Распределение кибератак по странам

доказательность), скрытность, территориальная независимость, доступность коммуникационных и ИТ-технологий. К слову, стать владельцем кибероружия дешевле, чем ядерного (например, на рис. 1 показано, что в топ-6 киберактивистов входят три неядерные страны, две из которых относятся к странам третьего мира). Такие аспекты легко использовать в рамках информационной войны вообще, например, предновогоднее «муссирование» влияния хакеров групп APT28 и APT29 на выборы в США[3]. При всем при этом ряд кибератак имеют весьма четко определённые черты и доказательную базу. К таким событиям можно отнести: опубликование каталога имплантатов АНБ [2], скандалы с закладками фирм-разработчиков программ (RSA, MS, HP и др.) и с троянскими программами в жестких дисках (фирм WD, ST, MT, SE и др.), с мероприятиями по разведпрограмме PRISM (с участием MS, FB, Google, Apple и др.) и, конечно, экономический шпионаж, приписываемый хакерской группе APT1 [3].

Очевидно, что основной вызов в сфере ИБ исходит от США, стремящихся к глобальному доминированию в киберпространстве. Такая позиция определена директивой президента США PDD 20, подкреплена действиями соответствующего рода войск (USCYBERCOM), технологической инфраструктурой (например, только датацентр АНБ – Utah Data Center – декларирует обработку 5 зеттабайт) и, соответственно, технологическим опережением [4, 5].

Анализу содержания требований информационной безопасности в нашей стране с учетом новых глобальных угроз и вызовов и посвящена данная работа.

2. Основные тенденции информационной безопасности в России

Одним из основных посылов нашей страны в глобальном политическом противоборстве, как известно, является реализация асимметричности подхода [6]. Не является исключением и область ИБ. Опираясь на системный подход, удобно рассмотреть следующие сегменты области ИБ нашей страны:

– *политические парадигмы;*
– *законодательство;*
– *нормативные требования;*
– *технологии;*
– *кадровые вопросы.*

2.1. Политические парадигмы

В плане политических парадигм в области ИБ следует выделить:

– *документальный уровень*, касающийся текущих доктрин национальной и информационной безопасности;

– *организационный уровень*, касающийся организационно-штатных структур (киберкомандование);

– *технологический* уровень – курс на импортозамещение.

Новый документальный уровень составляют прежде всего два концептуальных документа:

– «Стратегия национальной безопасности Российской Федерации до 2020 г.» от 31.12.2015[4],

– «Доктрина информационной безопасности Российской Федерации» от 05.12.2016[5].

В данных документах четко обозначены угрозы и риски в области высоких технологий и направления их снижения. При этом отмечены трудности

[3] https://ria.ru/world/20161230/1485006633.html

[4] http://www.scrf.gov.ru/documents/1/133.html

[5] http://www.scrf.gov.ru/documents/6/5.html

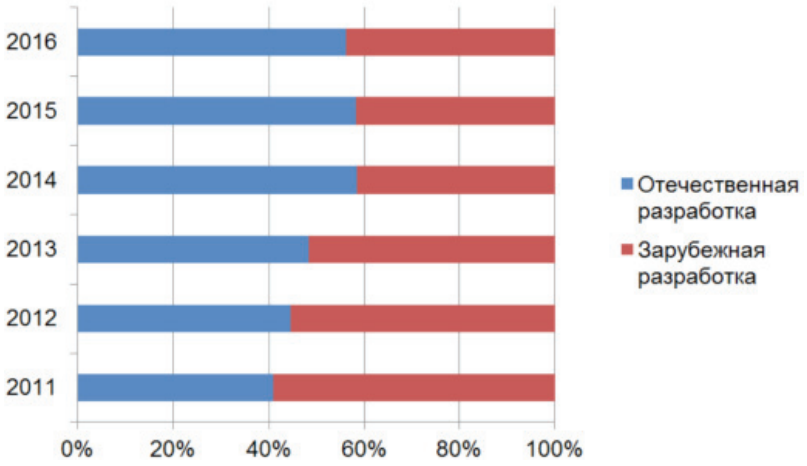


Рис. 2. Соотношение сертифицированных средств защиты информации

реагирования на угрозы в связи «со стремлением отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве».

Что касается создания киберкомандования, то об этой возможности были официальные заявления вице-премьера и министра обороны нашей страны несколько лет назад[6].

Задачи, связанные с курсом на импортозамещение именно в ИБ, явно обозначены пока лишь с программными изделиями, определенными в «Плане импортозамещения программного обеспечения до 2025 года»[7] и вносимыми в «Единый реестр российских программ для ЭВМ и БД»[8]. В то же время на текущий период имеется ряд послаблений, в том числе и собственно для регуляторов индустрии ИБ (ФСБ России, ФСТЭК России), что определено Постановлением Правительства РФ 18.07.2016 № 684[9]. Концептуальные вопросы модернизации электронной промышленности по понятным причинам находятся на этапе первичных решений [7]. На рис. 2 представлена статистика защищенных изделий, прошедших оценку согласно реестру ФСТЭК России.

2.2. Законодательство

В плане становления законодательства следует отметить следующие моменты:

– прекращение развития проекта «Концепции стратегии кибербезопасности РФ» [8];

– реализация Указа Президента РФ от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (ГосСОПКА [9]);

– ожидание ратификации проекта ФЗ «О безопасности критической информационной инфраструктуры РФ»[10] [10, 11].

Нельзя не отметить ряд законодательных актов по изменениям в Законе «О персональных данных», инициативы по кардинальному изменению Закона «О связи» и сопутствующих федеральных законов (149-ФЗ, 152-ФЗ, 184-ФЗ и др.), а также «пакет Яровой», которые касаются как обновления устарелых технологических концепций, так и повышения уровня госконтроля и национальной безопасности киберпространства (включая повышение информационной безопасности Рунета).

2.3. Нормативные требования

В плане формирования новых требований к мерам и средствам защиты информации (СЗИ) тон задает, без преувеличения, ФСТЭК России и Технический комитет по стандартизации ТК 362 «Защита информации». Выделим основные инновационные направления:

– формирование новых организационно-технических мер;

– определение новых критериев оценки СЗИ.

2.3.1. Формирование новых организационно-технических мер

Что касается организационно-технических мер, то в стране сосуществуют два параллельных подхода:

– меры, определенные международным законодательством, в частности ISO 27001 (14 мер);

[6] www.interfax.ru/russia/333123

[7] http://minsvyaz.ru/ru/documents/4548/

[8] https://reestr.minsvyaz.ru/reestr/

[9] http://publication.pravo.gov.ru/Document/View/0001201607210022

[10] http://www.slideshare.net/adorofeev/ss-60963690

– комплексы мер, определенные приказами ФСТЭК России №№ 17, 21, 31 (13, 15 и 21 мера соответственно).

Примеры мер, соответствующих международному и федеральному подходу представлены в табл. 1.

Таблица 1.

Организационно-технические меры безопасности

ISO 27001: 2013	Приказ ФСТЭК России №17
A.5: Политики информационной безопасности A.6: Организационные аспекты информационной безопасности A.7: Вопросы безопасности, связанные с персоналом A.8: Управление активами A.9: Управление доступом A.10: Криптография A.11: Физическая безопасность и защита от угроз окружающей среды A.12: Безопасность операций A.13: Безопасность коммуникаций A.14: Приемка, разработка и поддержка систем A.15: Отношения с поставщиками услуг A.16: Управление инцидентами информационной безопасности A.17: Аспекты информационной безопасности в обеспечении непрерывности бизнеса A.18: Соответствие требованиям	1. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) 2. Управление доступом субъектов доступа к объектам доступа (УПД) 3. Ограничение программной среды (ОПС) 4. Защита машинных носителей информации (ЗНИ) 5. Регистрация событий безопасности (РСБ) 6. Антивирусная защита (АВЗ) 7. Обнаружение вторжений (СОВ) 8. Контроль (анализ) защищенности информации (АНЗ) 9. Обеспечение целостности информационной системы и информации (ОЦЛ) 10. Обеспечение доступности информации (ОДТ) 11. Защита среды виртуализации (ЗСВ) 12. Защита технических средств (ЗТС) 13. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)

Наличие различных классов мер, конечно, создает некоторое противоречие и снижает уровень унификации организационно-технического базиса ИБ. Очевидно, уровень энтропии стандартизации еще повысится с внедрением неаутентичных стандартов (к примеру: новый стандарт *ИСО 27001 NEQ* не эквивалентен стандарту ISO 27001 в отличие от ИСО 27001).

Инновационность же подхода, предлагаемого приказами ФСТЭК России, состоит в попытке внедрения риск-ориентированного подхода (в реальности, квази-риск-ориентированного [12]) вместо директивного со всеми вытекающими преимуществами.

Еще одним значимым шагом в направлении оптимизации уровня ИБ следует считать разработку передовых национальных мер по безопасной разработке ПО (ГОСТ Р 56939-2016), которые направлены на выявление дефектов и уязвимостей на ранних стадиях жизненного цикла защищенных систем (рис. 3) [13].

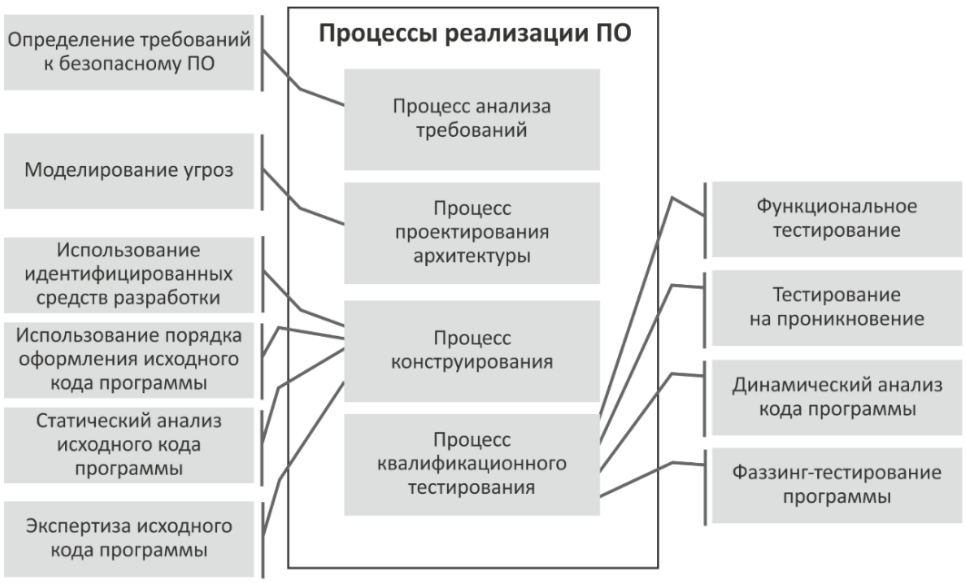


Рис. 3. Меры по реализации безопасных программ

2.3.2. Определение новых критериев оценки соответствия средств защиты информации

Как и с рассмотренными выше мерами безопасности, в стране сосуществуют два подхода и к оценке соответствия ИТ-продукции. Традиционный подход, определенный «Оранжевой книгой» (стандарты TCSEC, 1983 г.), представлен в нашей стране руководящими документами Гостехкомиссии России (1992-1999 гг.) и рядом специальных документов. Важно, что подход распространяется не только на СЗИ, но и на автоматизированные системы (*объекты информатизации*). Несмотря на простоту и апробированность, данный подход изживает себя по причине динамичности новых угроз и сложности программных средств и систем.

В мировом сообществе с середины 90-х годов прошлого века проходит апробацию подход «Общие критерии» (стандарты линейки ISO 15408) [14]. Данный подход позволяет, в первую очередь, создавать гибкие полуформальные (нотационные) нормативные документы, ориентированные на современные угрозы ИБ и учитывающие качество изделий. Опираясь на указанный подход, ФСТЭК России недавно разработала ряд нормативных правовых актов (НПА) и пакетов профилей защиты, задающих требования к следующим СЗИ:

– системам обнаружения вторжений;

– средствам антивирусной защиты;

– средствам доверенной загрузки;

– средствам контроля съемных машинных носителей информации;

– межсетевым экранам;

– операционным системам.

В текущем году ожидается появление требований по безопасности информации, предъявляемых к СУБД, базовым системам ввода-вывода (BIOS), средствам управления потоками информации, средствам защиты от несанкционированного вывода (ввода) информации (DLP-системам), средствам контроля и анализа защищенности, средствам идентификации и аутентификации, средствам управления доступом, средствам мониторинга событий безопасности (SIEM), средствам защиты среды виртуализации.

Новая классификация уровней защищенности информационных систем представлена в табл.2.

Таблица 2.

Классификация средств защиты информации

Классы защиты СЗИ	Класс защищенности ГИС	Уровень защищенности ИСПДн	Класс защищенности АСУ ТП
6	3, 4	3, 4	3
5	2	2	2
4	1	1	1
3	Применяются в информационных системах, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну		
2			
1			

К недостаткам подхода «Общих критериев» относят его сложность и – что касается нашей страны – дополнительные трудности его применения из-за недостатка специалистов и методической базы. Данный подход пока не применим для оценки соответствия объектов информатизации.

Следует указать, что наша страна не участвует в международных соглашениях по указанной тематике, что снижает уровень унификации и требует дополнительных усилий по доступу к накопленному международному опыту по тематике – в первую очередь к методической базе «Общих критериев», а также к отслеживанию кардинальных изменений [15].

2.3.3. Вектор на результативность

Как отмечалось, используемый директивный подход в динамичной ИБ-среде малоэффективен и малорезультативен [12]. Данная ситуация претерпела принципиальные изменения с 2016 г. благодаря инициативам ФСТЭК России. Нормативный прорыв в области результативности проверок по требованиям ИБ, в первую очередь, следует связать с внедрением передовых практик выявления уязвимостей согласно ISO 20004 (рис. 4.), а также с его поддержкой недавно созданным Банком данных угроз безопасности информации ФСТЭК России[11].

[11] http://bdu.fstec.ru/

Рис. 4. Этапы контроля уязвимостей в программных средствах по ISO 20004

Отметим особенности современной позиции ФСТЭК России:

– разрабатываемые документы «живые» (см. «План разработки НПА» на портале www.ftec.ru), т.е. подлежат периодическому обновлению (как известно, руководящие документы Гостехкомиссии России не претерпевали модификации с момента создания);

– разворот в сторону повышения результативности, включая тестирование на проникновение и анализ уязвимостей;

– поддержка Банка угроз и уязвимостей ФСТЭК России, получившего, фактически, национальный статус (рис. 5);

– конкретизация требований к лицензиатам, испытательным лабораториям и органам по сертификации.

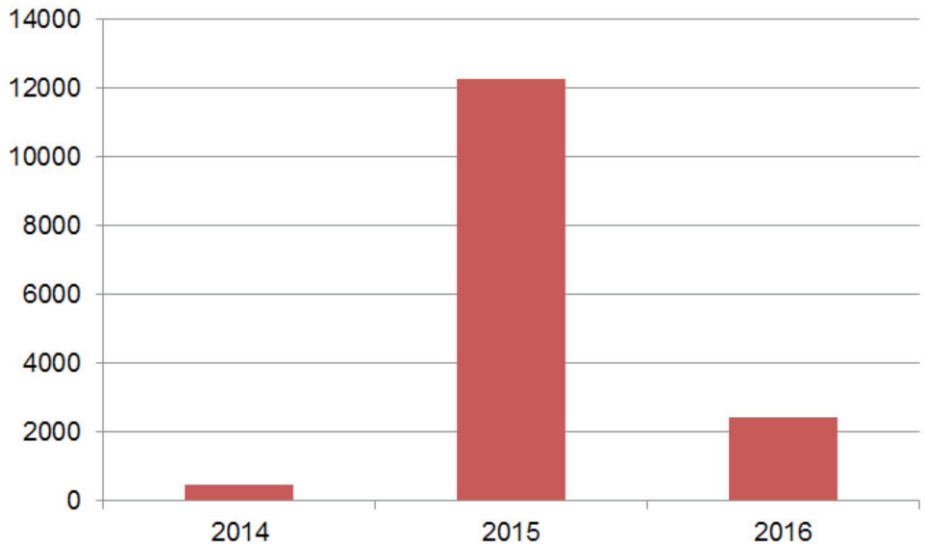


Рис. 5. Динамика пополнения Банка данных угроз безопасности информации ФСТЭК России по годам

2.3.4. Разработка национальных стандартов

Деятельность по стандартизации в области ИБ обеспечивается, главным образом, ТК 362 и ТК 26. Благодаря этим техническим комитетам в стране сложилась весьма представительная передовая нормативная база ИБ в виде банка международных и национальных стандартов. В табл. 3 представлены стандарты по ИБ за последние три года.

Таблица 3.

Новые стандарты по информационной безопасности

Номер стандарта	Название
ГОСТ Р ИСО/МЭК 27007-2014	ИТ. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента ИБ
ГОСТ Р ИСО/МЭК 27013-2014	ИТ. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1
ГОСТ Р ИСО/МЭК 27033-3-2014	ИТ. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления
ГОСТ Р ИСО/МЭК 27034-1-2014	ИТ. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия
ГОСТ Р ИСО/МЭК 27037-2014	ИТ. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме
ГОСТ Р 51583-2014	ЗИ. Порядок создания АС в защищенном исполнении. Общие положения
ГОСТ Р 56045-2014	ИТ. Методы и средства обеспечения безопасности. Рекомендации для безопасности аудиторов в отношении мер и средств контроля и управления ИБ
ГОСТ Р 56093-2014	ЗИ. АС в защищенном исполнении. Средства обнаружения преднамеренных силовых электромагнитных воздействий. Общие требования
ГОСТ Р 56103-2014	ЗИ. АС в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения
ГОСТ Р 56115-2014	ЗИ. АС в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования
ГОСТ Р 34.12-2015	ИТ. Криптографическая защита информации. Блочные шифры
ГОСТ Р 34.13-2015	ИТ. Криптографическая защита информации. Режимы работы блочных шифров
ГОСТ Р 56545-2015	ЗИ. Уязвимости информационных систем. Правила описания уязвимостей
ГОСТ Р 56546-2015	ЗИ. Уязвимости информационных систем. Классификация уязвимостей информационных систем
ГОСТ Р 56938-2016	ЗИ. Защита информации при использовании технологий виртуализации. Общие положения
ГОСТ Р 56939-2016	ЗИ. Разработка безопасного программного обеспечения. Общие требования

2.4. Технологии

В отечественных документах обозначено около двадцати механизмов (мер и средств) защиты информации. Однако согласно прогнозу Высшей школы экономики (ВШЭ) [16] выделяют три *перспективных* базовых направления развития механизмов безопасности, а именно:

– консолидация средств защиты информации;

– внедрение биометрических средств и методов безопасного доступа;

– исследование вопросов постквантовой криптографии.

Первое направление определяется тем, что развитие отдельных механизмов безопасности достигло своего технологического потолка в плане результативности. Наглядным примером является неэффективность применения средств антивирусной защиты и средств обнаружения вторжений (основанных на сигнатурных методах) для выявления целенаправленных вредоносных атак (APT-атак). Одним из путей вывода систем обеспечения ИБ на новый уровень результативности является организация сбора и корреляции событий от всех СЗИ и устройств с дальнейшим реагированием (управле-

нием) и оценкой соответствия [17]. Подобные решения получили название SIEM-системы.

Биометрические средства позволяют, с одной стороны, исключить недостатки, свойственные техническим средствам идентификации и аутентификации, а с другой – выйти на уровень верификации субъектов защищенных информационных систем [18].

Постквантовая криптография – инновационное направление, основанное на эффектах квантовой физики, в первую очередь, сверхвысокой производительности квантового компьютера и невозможностью перехвата квантовой передачи данных [19].

2.5. Кадровые вопросы

Кадровые вопросы традиционно являются первостепенными в области ИБ из-за социальной составляющей самого понятия ИБ, а безопасность персонала относят к самому уязвимому звену защищенных систем. В общем плане можно констатировать, что в стране продолжает функционировать ассоциация вузов в области информационной безопасности, а также идет совершенствование профессиональных стандартов в этой области [20]. Регуляторы ИБ, в свою очередь, продолжают конкретизацию требований к лицензиатам (табл. 4). С другой стороны, в стране пока нет национальной сертификации специалистов по ИБ.

Таблица 4.

Требования по обучению

Вид и методы защиты информации	Законодательная база	Требования к лицензиатам
Защита государственной тайны	Методические рекомендации ФСБ России и ФСТЭК России	ВПО по ЗИ или ВТО и переподготовка или повышение квалификации по вопросам защиты информации
Средства криптографической защиты информации	ПП 313	ВПО или переподготовка (1000, 500, 100 час.) с учетом стажа специалиста
Техническая защита конфиденциальной информации	ПП 79, 171 (с 15.06.2017 г.)	ВПО или переподготовка 360/500 час (руководители), 250/100 (работники) с учетом стажа специалиста; переподготовка (72 час.) один раз в пять лет

3. Выводы

Современные вызовы и угрозы в области информационной и кибербезопасности страны обусловливают потребности в постоянном совершенствовании развития данной отрасли, в том числе путем изучения передового международного опыта.

В нашей стране за последние несколько лет произошли серьезные нормативно-правовые изменения в направлении отказа от директивного подхода, главным образом, путем внедрения риск-ориентированного подхода, гибких нормативных требований по линии «Общих критериев», а также повышения результативности проверок, связанных с оценкой основных факторов безопасности (дефектов, уязвимостей, угроз). В настоящее время такой подход инициирован и проходит масштабную апробацию под эгидой ТК 362 и ФСТЭК России.

В то же время в стране остается ряд проблемных вопросов законодательного, нормативного, технологического и кадрового характера, решение которых видится в недалеком будущем благодаря нарабатываемому потенциалу отрасли.

Рецензент: *Федичев Андрей Валерьевич, кандидат технических наук, директор ФБУ «Научный центр правовой информации» при Минюсте России, Москва.*

E-mail: fedichev@scli.ru

Литература

1. Плигин В.Н., Макаренко Г.И. Страна нуждается в обновлении общественных договоров в современном российском обществе // Мониторинг правоприменения. 2015. № 1 (14). С. 4–11.
2. Клянчин А.И. Каталог закладок АНБ (Spigel). Часть 1. Инфраструктура // Вопросы кибербезопасности. 2014. № 2 (3). С. 60–65.
3. Марков А.С. Летописи кибервойн и величайшего в истории перераспределения богатства // Вопросы кибербезопасности. 2016. № 1 (14). С. 68–74.
4. Голов И.Ю. Стратегический план научных исследований и разработок США в области кибербезопасности // Вопросы защиты информации. 2013. № 3 (102). С. 86–91.
5. Петренко А.А., Петренко С.А. НИОКР Агентства DARPA в области кибербезопасности // Вопросы кибербезопасности. 2015. № 4 (12). С. 2–22.
6. Любарец А.В. Ответная философская и геополитическая парадигма В.В.Путина // Актуальные проблемы гуманитарных и естественных наук. 2016. № 7-1. С. 229–231.
7. Муравник В.Б., Захаренков А.И., Добродеев А.Ю. Некоторые предложения по подходу и порядку реализации политики и стратегии импортозамещения в интересах национальной безопасности и укрепления обороноспособности Российской Федерации // Вопросы кибербезопасности. 2016. № 1 (14). С. 2–8.
8. Гаттаров Р.У. Концепция стратегии кибербезопасности // Вопросы кибербезопасности. 2014. № 1 (2). С. 2–4.
9. Петренко С.А., Курбатов В.А., Бугаев И.А., Петренко А.С. Когнитивная система раннего предупреждения о компьютерном нападении // Защита информации. Инсайд. 2016. № 3 (69). С. 74–82.
10. Генгринович Е.Л. Информационная безопасность критической инфраструктуры // Автоматизация в промышленности. 2015. № 2. С. 61–63.
11. Массель Л.В., Воропай Н.И., Сендеров С.М., Массель А.Г. Киберопасность как одна из стратегических угроз энергетической безопасности России // Вопросы кибербезопасности. 2016. № 4 (17). С. 2–10.
12. Марков А.С., Шеремет И.А. Теоретические аспекты сертификации средств защиты информации // Оборонный комплекс – научно-техническому прогрессу России. 2015. № 4 (128). С. 7–15.
13. Barabanov A.V., Markov A.S., Tsirlov V.L. Methodological Framework for Analysis and Synthesis of a Set of Secure Software Development Controls // Journal of Theoretical and Applied Information Technology. 2016. V. 88. N 1, pp. 77-88.
14. Барабанов А.В., Марков А.С., Цирлов В.Л. Оценка соответствия средств защиты информации «Общим критериям» // Информационные технологии. 2015. Т. 21. № 4. С. 264–270.
15. Chuzel J., Weber J., Huisman R. Medium and higher assurance evaluations in the European context. In Proceedings of the 16th International Common Criteria Conference (London, UK, Sep. 22-24, 2015). ICCC-2015. CESG, URL: https://www.iccc15.org.uk/Programme.aspx.
16. Прогноз научно-технологического развития России: 2030 / Под ред. Л.М.Гохберга и др. М.: Минобрнауки России, ВШЭ, 2014. 244 с.
17. Марков А., Фадин А. Конвергенция средств защиты информации // Защита информации. Инсайд. 2013. № 4 (52). С. 80–81.
18. Арутюнов В.В. О монографии «Биометрия на службе защиты информации». В сборнике: Современные проблемы и задачи обеспечения информационной безопасности. Труды Международной научно-практической конференции «СИБ-2014». Ответственный редактор О.А. Макарова. 2014. С. 165–168.
19. Корольков А.В. О некоторых прикладных аспектах квантовой криптографии в контексте развития квантовых вычислений и появления квантовых компьютеров // Вопросы кибербезопасности. 2015. 1 (9). С. 6–13.
20. Белов Е.Б., Лось В.П. О разработке профессиональных стандартов в области информационной безопасности // Доклады Томского государственного университета систем управления и радиоэлектроники. 2014. № 2 (32). С. 327–331.