РЕЦЕНЗИЯ НА КНИГУ «СЕМЬ БЕЗОПАСНЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

Петренко С.А.[1]

В самом начале 2017 года вышла в свет книга «Семь безопасных информационных технологий / А.В. Барабанов, А.В. Дорофеев, А.С. Марков, В.Л. Цирлов; под ред. А.С. Маркова. – М.:ДМК Пресс, 2017. – 224 с.», подготовленная группой авторов, успешно сочетающих научную и практическую работу, лидеров предприятия АО «НПО-Эшелон».

Темпы развития современных информационных и коммуникационных технологий («облачных» и мобильных, аппаратных и программных гипервизоров, больших данных *Big Data* и прогнозной аналитики *Big Data Analytics*, программно-конфигурируемых сетей *SDN* и виртуализации сетевых функций *NFV*, индустриального Интернета IIoT и Интернета вещей *IoT* и пр.) значительно опережают темпы разработки отечественной нормативно-правовой базы в области информационной безопасности.

DOI: 10.21681/2311-3456-2017-1-67-72

Поэтому вопрос, *«как обеспечить надлежащий уровень информационной безопасности предприятия», – обязательно влечет за собой следующие: в соответствии с какими критериями и показателями необходимо оценивать информационную безопасность, как планировать и управлять информационной безопасностью, как экономически оправдать организационные и технические мероприятия обеспечения информационной безопасности?* Вследствие этого, в дополнение к хорошо известным требованиям регуляторов, приходится использовать так называемые лучшие практики международных стандартов (ISO 38500, 27001, 9001, 15408, 22301, 27031, CobIT и пр.). В том числе, *методики количественного анализа рисков, планирования и управления экономической эффективностью инвестиций* в защиту информации.

В настоящее время в технологически развитых странах мира появилось новое поколение стандартов информационной безопасности, посвященных *практическим вопросам обеспечения и аудита информационной безопасности*. Это прежде всего международные и национальные стандарты оценки и *управления информационной безопасностью ISO 38500, 27001, 9001, 15408, 22301, 27031; стандарты аудита информационных систем и информационной безопасности COBIT, SAC, COSO, SAS 55/78* и некоторые другие, аналогичные им. В соответствие с этими стандартами обеспечение информационной безопасности в любой компании предполагает следующее. *Во-первых*, определение целей и задач обеспечения информационной безопасности. *Во-вторых*, создание эффективной системы управления информационной безопасностью. *В-третьих*, расчет совокупности детализированных не только качественных, но и количественных показателей информационной безопасности. *В-четвертых*, применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния. *В-пятых*, использование методик (с обоснованной системой *метрик и мер обеспечения информационной безопасности*) проведения аудита информационной безопасности, позволяющих объективно оценить текущее состояние дел.

Новое поколение стандартов отличается как от предыдущего, так и от хорошо известных руководящих документов ФСТЭК России, *большей формализацией аудиторской деятельности и более детальным комплексным учетом качественно и количественно проверяемых показателей* информационной безопасности компании. Комплексный учет показателей предполагает комплексный подход к аудиту, когда на соответствие определенным правилам проверяется не только *программно-техническая* составляющая информационной безопасности компьютер-

1 Петренко Сергей Анатольевич, доктор технических наук, профессор, Университет Иннополис, г. Иннополис, Татарстан, Россия. s.petrenko@rambler.ru

ной системы, но и *организационно-административные меры* по ее обеспечению.

В совокупности, такой подход к обеспечению информационной безопасности отечественных государственных и коммерческих предприятий позволяет:

• произвести *количественную оценку* текущего уровня безопасности, задать допустимые уровни рисков, разработать план мероприятий по обеспечению требуемого уровня безопасности на организационно-управленческом, технологическом и техническом уровнях с использованием современных методик и средств;

• рассчитать и *экономически обосновать* перед руководством или акционерами размер необходимых вложений в обеспечение безопасности на основе технологий анализа рисков, соотнести расходы на обеспечение безопасности с потенциальным ущербом и вероятностью его возникновения;

• выявить и *провести первоочередное блокирование* наиболее опасных уязвимостей до осуществления атак на уязвимые ресурсы;

• определить *функциональные отношения и зоны ответственности* при взаимодействии подразделений и лиц по обеспечению информационной безопасности предприятия, создать необходимый пакет организационно-распорядительной документации;

• разработать и согласовать со службами организации, надзорными органами *проект внедрения необходимых комплексов защиты*, учитывающий современный уровень и тенденции развития информационных технологий;

• обеспечить поддержание внедренного комплекса защиты в соответствии изменяющимся условиям работы организации, регулярными доработками организационно-распорядительной документации, модификацией технологических процессов и модернизацией технических средств защиты.

Актуальность книги подтверждается основными положениями новой *Доктрины информационной безопасности Российской Федерации* (утверждена Указом Президента Российской Федерации от 5 декабря 2016 № 646), которая развивает основные положения современной *Концепции внешней политики Российской Федерации* (утверждена Указом Президента Российской федерации от 30 ноября 2016 г. № 640) в области информационной безопасности.

Ориентация учебного материала книги на выполнение основных положений новой *Доктрины информационной безопасности Российской Федерации* крайне важна и своевременна. Дело в том, что предыдущая Доктрина информационной безопасности Российской Федерации, принятая еще в 2000 году, уже заметно устарела. В связи с этим потребовалась разработка нового документа, адекватного современному уровню развития информационных и коммуникационных технологий. Кроме того, за прошедшие 17 лет список актуальных угроз информационной безопасности заметно расширился, изменились взаимоотношения на мировой арене, несравнимо большими стали возможности киберпротивников. Более того, угрозы информационной безопасности вышли на уровень межгосударственного противостояния. При этом такие понятия как информационные операции, программно-аппаратные и психологические воздействия стали реальностью современных международных отношений.

По сравнению с прошлой редакцией Доктрины (2000г.) и вариантом новой Доктрины, обсуждавшейся в Совете Безопасности РФ летом 2016 года, текст утвержденной Доктрины информационной безопасности Российской Федерации был существенно дополнен и переработан. Новая Доктрина отличается четкой структурой и содержит: требуемый набор основных понятий (*национальные интересы РФ в информационной сфере, информационная безопасность РФ, угроза информационной безопасности РФ, система обеспечения информационной безопасности РФ, критическая информационная инфраструктура РФ и др.*); изложение национальных интересов России в информационной сфере; перечень основных угроз и оценку состояния информационной безопасности Российской Федерации; описание стратегических целей и основных направлений обеспечения информационной безопасности государства; описание организационных основ обеспечения информационной безопасности Российской Федерации. От прошлой Доктрины документ отличается краткостью, четкостью изложения, и в то же время широтой охвата рассматриваемых вопросов. В том числе, впервые сформулированы задачи доведения до российской и международной общественности достоверной информации о государственной политике РФ и ее официальной позиции по социально значимым событиям в стране и мире, задачи повышения защищенности критической информационной инфраструктуры (ст.23), ликвидации зависимости отечественной промышленности от зарубежных информационных технологий и средств обеспечения ИБ (ст.25),

поддержки инновационного и ускоренного развития системы обеспечения ИБ, отрасли ИТ и электронной промышленности (ст.26).

Авторами книги рассмотрены все основные разделы учебной литературы по подготовке и сдаче известных *международных сертификационных экзаменов в области информационной безопасности: CISSP (Certified Information Systems Security Professional), CSSLP (Certified Secure Software Lifecycle Professional), поддерживаемых международным консорциумом (ISC)2 – International Information Systems Security Certification Consortium; CISM (Certified Information Security Manager), CISA (Certified Information Systems Auditor), организуемых международной ассоциацией ISACA (Information Systems Audit and Control Association*), а именно:

1. ***Менеджмент информационной безопасности***. В этом разделе введены базовые понятия менеджмента информационной безопасности. Детально рассмотрены основные *этапы жизненного цикла СМИБ* на примере процессной модели *PDCA – «Plan (планирование), Do (реализация), Check (проверка) – Act (совершенствование)»*, получившей название *цикл Шухарта–Деминга*. В том числе, показана специфика разработки политик, регламентов и процедур ИБ на стадии планирования и особенности оценки информационных рисков. Рассмотрено, как на стадиях:

– *реализации* - осуществляется внедрение и поддержка политики ИБ, обработка рисков, осуществление контрмер, установка защитных средств и сервисов;

– *проверки* - выполняется контроль факторов ИБ, оценка и анализ эффективности процессов управления ИБ;

– *совершенствования* - реализуется выработка и принятие корректирующих и превентивных действий, проводятся переоценка рисков, пересмотр политики и т. д.

2. ***Обеспечение безопасного доступа***. В этом разделе показано, что *управление доступом (access control)* является одной из ключевых задач ИБ. Обращено внимание на то, что понятие управления доступом в рамках международных учебных курсов носит более широкий смысл, чем просто санкционированное разграничение доступа, и включает аспекты организации безопасного доступа пользователя к ресурсам системы вообще, например: с учетом защиты от вредоносных программ, легитимной деятельности пользователей, заданной готовности или восстанавливаемости системы. Рассмотрены все *основные категории и особенности управления доступом* на практике. Приведены основные типы средств идентификации и аутентификации. Рассмотрены особенности реализации известных протоколов сетевого доступа. Выделены отличия *дискреционного, мандатного и ролевого методов управления доступом*.

3. ***Обеспечение сетевой безопасности***. Здесь представлены основные типы и архитектуры компьютерных сетей, особенности реализации методов доступа к среде передачи данных, типовые сетевые спецификации. Подробно рассмотрена *базовая эталонная модель взаимодействия открытых систем* на практике. Показаны ключевые архитектурные особенности *стека протоколов TCP/IP* на практике. Представлена типовая классификация средств обеспечения сетевой безопасности.

4. ***Криптографическая защита информации***. В этом разделе приведены базовые понятия и методы криптографической защиты информации. Подробно рассмотрены *криптографические примитивы: симметричные криптосистемы, криптосистемы с открытым ключом, криптографические хэш-функции, электронные подписи; цифровые сертификаты*. Показаны особенности реализации *симметричного и асимметричного шифрования* на практике.

5. ***Разработка безопасных программ***. Подробно рассмотрена специфика различных *концептуальных моделей жизненного цикла: модель отладки, V-образная (через классы тестирования), каскадная (последовательная, детерминированная), каскадная с промежуточным контролем и обратной связью, инкрементальная (последовательная), итерационная (версионная), гибкая (agile), спиральная (PDCA-модель ПО) и др*. Рассмотрена практика реализации безопасного жизненного цикла программного обеспечения. Приведены рекомендации для проектирования архитектуры безопасного программного обеспечения.

6. ***Моделирование и оценка соответствия***. Здесь рассмотрены базовые понятия, определяющие безопасную архитектуру с концептуальной точки зрения: *доверенная среда; доверенный маршрут передачи данных; периметр безопасности; монитор безопасности; ядро безопасности. Показаны особенности реализации доверенной средой вычислений (Trusted Computing Base,TCB),* под которой понимается совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения выполнения политик ИБ – подмножество защищаемой информационной системы, обеспечивающее защиту

информации и выполнение требований, установленных политиками ИБ. Показаны отличия известных моделей управления доступом. Рассмотрены принципы безопасной архитектуры ЭВМ. Подробно рассмотрены обязательные процедуры оценки соответствия.

7. ***Обеспечение непрерывности бизнеса и восстановления***. В этом разделе подробно рассмотрены две составные части *менеджмента непрерывности бизнеса*: планирование непрерывности бизнеса (*Business Continuity Planning, BCP*); планирование аварийного восстановления после аварий (*Disaster Recovery Planning, DRP*). Рассмотрена специфика решения задач:

– *планирования (Plan)* - подготовка планирования, оценка влияния прерываний на бизнес, определение стратегий обеспечения непрерывности бизнеса, разработка документации, определение необходимости внедрения мер ИБ (controls) для минимизации остаточных рисков;

– *исполнения (Do)* - внедрение разработанных документов и необходимых технических решений; обучение персонала;

– *проверки (Check)* - тестирование разработанных планов;

– *действия/исправления (Act)* - исправление выявленных в ходе тестирования проблем; совершенствование системы BCM.

В приложениях книги представлен свод типовых компьютерных атак, а также почитаемые за рубежом этические правила, раскрывающие рассмотренные международные принципы ИБ.

Представленный материал книги в совокупности определяют значительный **вклад авторов** в *прикладные вопросы теории защиты информации*.

Тема книги и направленность изложенных вопросов соответствует специальности *05.13.19 – «Методы и системы защиты информации, информационная безопасность»*:

п. 1. Теория и методология обеспечения информационной безопасности и защиты информации;

п. 3. Методы и модели выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса;

п. 9. Модели и методы оценки защищенности информации и информационной безопасности объекта;

п. 5. Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет;

п. 11. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа;

п. 13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности и др.

Материалы книги были *апробированы в образовательной деятельности* МГТУ им. Н. Э. Баумана (курс «Сертификация специалистов по информационной безопасности»), в Финансовом университете при Правительстве РФ (курс «Организационные основы информационной безопасности») и в Учебном центре «Эшелон» (курс «Подготовка к CISSP за 12 сиреневых вечеров»). Также материалы книги апробированы *в научно-исследовательской деятельности* авторов книги по направлениям:

– анализ безопасности программных ресурсов, в т.ч. веб-приложений,

– аудит безопасности исходного кода (поиск уязвимостей),

– аудит защищенности компьютерных систем и сетей,

– аудит защищенности автоматизированных систем управления технологическими процессами,

– анализ защищенности беспроводных сетей,

– доверенная загрузка операционных и виртуальных сред,

– разработка распределенных систем по управлению ложными сетевыми объектами и ловушками (honeypot),

– разработка систем обнаружение вторжений,

– создание программно-аппаратных межсетевых экранов,

– оценка и контроль эффективности система защиты от утечек данных и др.

В качестве *замечаний и рекомендаций* по книге стоит отметить следующее. В настоящее время большинством российских компаний определены следующие приоритетные задачи развития и совершенствования своей деятельности:

– минимизация рисков бизнеса путем защиты своих интересов в информационной сфере;

– обеспечение безопасного, доверенного и адекватного управления предприятием;

– планирование и поддержка непрерывности бизнеса;

– повышение качества деятельности по обеспечению информационной безопасности;

– снижение издержек и повышение эффективности инвестиций в информационную безопасность;

– повышение уровня доверия к компании со стороны акционеров, потенциальных инвесторов, деловых партнеров, профессиональных участников рынка ценных бумаг, уполномоченных государственных органов и других заинтересованных сторон.

Здесь успешное выполнение перечисленных задач в условиях воздействия внутренних и внешних факторов, а также действий конкурентов и злоумышленников проблематично. Поэтому важно учитывать следующее:

– в разрабатываемых политиках безопасности отечественных компаний необходимо учитывать в равной мере нормативные, экономические, технологические, технические и организационно-управленческие аспекты планирования информационной безопасности и управления ею. Только в этом случае можно достигнуть разумного баланса между стоимостью и эффективностью разрабатываемых правил политик безопасности. При этом упомянутые политики безопасности не должны противоречить отечественной нормативной базе в области защиты информации, в том числе нормативно-правовым документам (федеральным законам, указам Президента, постановлениям Правительства) и нормативно-техническим документам;

– желательно учитывать текущие реформы действующей Государственной системы стандартизации (ГСС) согласно Федеральному закону № 184-ФЗ «О техническом регулировании», рекомендации ГОСТ Р ИСО/МЭК 15408, рекомендации функционального стандарта ГОСТ Р 51583-2014, описывающего этапность построения защищенных информационных систем, рекомендации ФСТЭК России для выработки требований по технической защите конфиденциальной информации;

– при отражении нормативного аспекта рекомендуется следовать требованиям новой российской национальной системы стандартизации, основанной на системе технического регулирования в соответствии с рекомендациями Федерального закона № 184-ФЗ «О техническом регулировании». Это отвечает последним веяниям формирования в Российской Федерации технического законодательства, обеспечивающего выполнение Соглашений Всемирной торговой организации (ВТО) по техническим барьерам в торговле (ТБТ) и санитарным и фитосанитарным мерам (СФС) с учетом принципов нового подхода к технической регламентации в Европейском союзе (ЕС).

– при отражении экономического подхода к планированию информационной безопасности и управлению ею на основе концепции управления рисками рекомендуется обратить внимание на методы: прикладного информационного анализа (Applied Information Economics, AIE); расчета потребительского индекса (Customer Index, CI); расчета добавленной экономической стоимости (Economic Value Added, EVA); определения исходной экономической стоимости (Economic Value Sourced, EVS); управления портфелем активов (Portfolio Management, PM); оценки действительных возможностей (Real Option Valuation, ROV); поддержки жизненного цикла искусственных систем (System Life Cycle Analysis, SLCA); расчета системы сбалансированных показателей (Balanced Scorecard, BSC); расчета совокупной стоимости владения (Total Cost of Ownership, TCO); функционально-стоимостного анализа (Activity Based Costing, ABC). В частности, для расчета расходной части на техническую архитектуру обеспечения информационной безопасности рекомендуется использовать метод совокупной стоимости владения (TCO), а для обоснования инвестиций в корпоративную систему защиты информации – методы ожидаемых потерь, оценки свойств системы безопасности, а также анализа дерева ошибок. При этом следует учитывать, что только метод ожидаемых потерь позволяет получить количественную оценку стоимости и выгод от контрмер безопасности;

– при разработке системного облика проектов безопасности в отечественных компаний целесообразно воспользоваться стандартами BSI IT Protection Manual (www.bsi.de), NIST США серии 800 (www.nist.gov) CIS (www.cisecurity.org), NSA (www.nsa.gov).

Однако перечисленные замечания и рекомендации носят частный характер и не оказывают существенного влияния на общую положительную оценку книги. В целом книга представляет собой логически завершенный методологический труд, в котором достаточно полно раскрыты практические вопросы менеджмента информационной безопасности на основе лучшей международной практике. Материал книги изложен грамотно, логически последовательно и сопровождается интересными примерами и контрольными вопросами, а также оригинальными рисунками.

Вывод. Книга «*Семь безопасных информационных технологий / А.В. Барабанов, А.В. Дорофеев, А.С. Марков, В.Л. Цирлов; под ред. А.С. Маркова. – М.: ДМК Пресс, 2017. – 224 с.*» написана на актуальную тему, отличается практической значимостью и имеет завершенный характер.

Упомянутая книга подготовлена на основе материалов известных *международных сертификационных экзаменов* в области информационной безопасности, адаптированных под отечественную специфику обеспечения информационной безопасности.

Авторами книги являются известные отечественные специалисты в области информационной безопасности.

По мнению рецензента, книга является первым полным русскоязычным практическим руководством по подготовке и сдаче *международных сертификационных экзаменов CISSP и CSSLP (ISC)2, а также CISM и CISA ассоциации ISACA* и выгодно отличается от других источников, преимущественно изданных за рубежом, тем, что в ней последовательно изложены все основные принципы, подходы, методы и методики управления информационной безопасностью, специальным образом адаптированные для практики отечественных предприятий.

Эта книга может быть полезна следующим основным группам читателей:

– руководителям служб автоматизации (CIO) и служб информационной безопасности (CISO), ответственным за организацию режима секретности, адекватного текущим целям и задачам бизнеса компании;

– внутренним и внешним аудиторам, которым приходится комплексно оценивать текущее состояние системы менеджмента информационной безопасности предприятия на соответствие некоторым национальным и международным стандартам, *например ISO 27001, 9001, 15408, 22301, 27031, COBIT, SAC, COSO, SAS 55/78 и пр.*;

– менеджерам высшего эшелона управления компанией (TOP-менеджерам), которым приходится разрабатывать и внедрять систему менеджмента информационной безопасности предприятия;

– администраторам безопасности, системным и сетевым администраторам, администраторам БД, которые отвечают за соблюдение правил безопасности в отечественных корпоративных информационных системах.

Книга также может использоваться в качестве учебного пособия студентами и аспирантами соответствующих технических специальностей, тем более что материалы многих глав основаны, в том числе, и на опыте преподавания авторов книги в МГТУ им. Н.Э.Баумана и Финансовом университете при Правительстве РФ.

BOOK REVIEW: SEVEN INFORMATION SECURITY TECHNOLOGIES

Petrenko S.A.[2]

The book is the first full guidance manual in Russian for preparing for and taking exams for international certificates CISSP as well as CISM and CISA (ISACA). The main advantages of the book in comparison with other sources that are mainly published abroad is that it consistently describes the main principles, approaches, methods and procedures for managing information security, which are specially adapted for practical use by the Russian audience! This CISSP–guide is an excellent manual for those, who want to be successful in information security and increase its professional status in accordance with the international requirements. The authors chose the study topics that provide maximum coverage of the requirements to the applicants for CISSP. The book gives many interesting pictures, positive questions with answers on each topic, many original classifications and explanations of the terms in English. The book is well–structured and is easy to read. It provides short comparison of international practices with the national reality for the Russian reader.

2 Sergey Petrenko, Dr.Sc., Professor, University of Innopolis, Innopolis, Tatarstan, Russia. s.petrenko@rambler.ru