

Содержание

Предисловие о семи безопасных информационных технологиях	6
Глава 1. Менеджмент информационной безопасности.....	9
1.1. Основные понятия информационной безопасности.....	9
1.2. Система менеджмента информационной безопасности	12
1.3. Анализ и управление рисками.....	17
1.4. Классификация информации.....	23
1.5. Порядок использования политик, стандартов и руководств.....	28
1.6. Особенности работы с персоналом	31
Вопросы для повторения.....	33
Лабораторная работа	36
Глава 2. Обеспечение безопасного доступа	38
2.1. Понятие управления безопасным доступом	38
2.2. Категории управления доступом	39
2.3. Свойство подотчетности и подсистемы управления доступом.....	41
2.4. Средства идентификации и аутентификации	43
2.5. Протоколы сетевого доступа	54
2.6. Методы управления доступом.....	58
Вопросы для повторения.....	61
Лабораторная работа	64
Глава 3. Обеспечение сетевой безопасности.....	65
3.1. Понятие компьютерной сети.....	65
3.2. Базовая эталонная модель взаимосвязи открытых систем.....	74
3.3. стек протоколов TCP/IP	78
3.4. Средства обеспечения сетевой безопасности	91
Вопросы для повторения.....	101

Глава 4. Криптографическая защита информации	106
4.1. Основные криптографические примитивы	106
4.2. Элементарное шифрование.....	108
4.3. Симметричная криптография	114
4.4. Асимметричная криптография	118
4.5. Электронно-цифровая подпись и криптографическая хэш-функция.....	123
4.6. Инфраструктура открытых ключей	127
Вопросы для повторения.....	128
Глава 5. Разработка безопасных программ.....	132
5.1. Модели жизненного цикла программного обеспечения.....	132
5.2. Безопасный жизненный цикл программного обеспечения	136
5.3. Обзор мер по разработке безопасного программного обеспечения	143
Вопросы для повторения.....	154
Глава 6. Моделирование и оценка соответствия	158
6.1. Основные понятия безопасной архитектуры	158
6.2. Концептуальные модели управления доступом	160
6.3. Принципы безопасной архитектуры ЭВМ	166
6.4. Скрытые каналы передачи информации.....	170
6.5. Критерии оценки соответствия.....	173
Вопросы для повторения.....	184
Глава 7. Обеспечение непрерывности бизнеса и восстановления.....	187
7.1. Управление непрерывностью бизнеса и восстановлением	187
7.2. Модель менеджмента непрерывности бизнеса	188
Вопросы для повторения.....	198
Литература.....	201
Ответы на вопросы для повторения.....	208

Приложение 1. Кодекс профессиональной этики	214
Четыре заповеди профессиональной этики (ISC)2	214
Семь правил профессиональной этики ISACA	214
Приложение 2. Типовые компьютерные атаки	216
Криптографические и парольные атаки.....	216
Атаки на отказ в обслуживании	217
Атаки на программный код и приложения	218
Атаки социальной инженерии и физические атаки	219
Сетевые атаки	220

Предисловие о семи безопасных информационных технологиях

Держите меня всемером!

План безопасности Белоснежки

Безопасные информационные технологии (опираясь на ISO/IEC 38500-2015) можно определить как методические и технические ресурсы, необходимые для безопасного сбора, обработки, хранения и распространения информации в компьютерных системах.

Чрезвычайная актуальность и удивительный интерес к тематике не нуждаются в аргументации. Внедрение безопасных информационных технологий (ИТ) — сейчас самое передовое направление автоматизации любой деятельности.

В настоящее время известен ряд увлекательных учебников в области информационной безопасности (ИБ), отражающий академические изыскания отечественных научных школ или ИТ-корпораций [1–40]. Особенностью этой книги является формирование учебного курса, соответствующего исключительно *международному* вектору развития в области обучения ИБ, проще говоря, неофициальному осмыслению самых востребованных в мире *сертификационных курсов в области ИБ*, к примеру:

- ◇ CISSP (Certified Information Systems Security Professional), CSSLP (Certified Secure Software Lifecycle Professional), поддерживаемых международным консорциумом (ISC) — International Information Systems Security Certification Consortium [41–46];
- ◇ CISM (Certified Information Security Manager), CISA (Certified Information Systems Auditor), организуемых международной

ассоциацией ISACA (Information Systems Audit and Control Association) и др. [47–51].

Определение авторами указанной, в общем-то принципиальной, позиции связано с двумя моментами:

- ◇ данный учебник исключительно полезен *активным ИТ-специалистам*, чтобы подготовиться к соответствующим международным сертификационным экзаменам в области ИБ, что чрезвычайно важно в карьерном и информационно-публичном плане;
- ◇ понимание специфики элитных международных курсов позволяет российским профессионалам провести некоторую рефлексию отечественных направлений в обучении по линии ИБ, сравнить их с системой взглядов, предпочитаемой зарубежными специалистами.

Надо понимать, что изучение международных тенденций в безопасных информационных технологиях позволяет отечественным ИТ-стартапам повысить свою конкурентоспособность на международных рынках.

Разумеется, авторами учебника выступили специалисты, имеющие соответствующие сертифицированные международные статусы:

- ◇ Барабанов Александр (CISSP, CSSLP);
- ◇ Дорофеев Александр (CISSP, CISA, CISM, BSI Lead Auditor);
- ◇ Марков Алексей (CISSP, SBCI, BSI Lead Auditor, IEEE Member, ACM Member);
- ◇ Цирлов Валентин (CISSP, CISM, AMBCI).

Учебные материалы апробированы в МГТУ им. Н. Э. Баумана (курс «Сертификация специалистов по информационной безопасности»), в Финансовом университете при Правительстве РФ (курс «Организационные основы информационной безопасности») и в УЦ «Эшелон» (курс «Подготовка к CISSP за 12 сиреневых вечеров»). Отдельные вопросы обсуждались на страницах рецензируемого журнала «Вопросы кибербезопасности» [52–61].

Учебник включает в себя семь разделов по безопасным информационным технологиям:

- 1) менеджмент информационной безопасности;
- 2) обеспечение безопасного доступа;
- 3) обеспечение сетевой безопасности;
- 4) криптографическая защита информации;
- 5) разработка безопасных программ;
- 6) моделирование и оценка соответствия;
- 7) обеспечение непрерывности бизнеса и восстановления.

В качестве приложений к учебнику представлен свод типовых компьютерных атак, чтоб исключить их повторяемость в различных главах, а также декларируемые за рубежом этические правила, что поможет понять некоторые идейные международные принципы ИБ.

Выбор указанных разделов определен опытом успешной сдачи названных ранее сертификационных экзаменов. Разделы дополнены оригинальными вопросами и заданиями для самоподготовки.

Авторы в книге придерживаются международной терминологии, определенной международными стандартами или сертификационными курсами, специфические термины продублированы на английском языке.

Авторы выражают благодарность сотрудникам НПО «Эшелон»: сертифицированным специалистам CISSP Андрею Фадину и CISSP Евгению Веселову (за моральную поддержку), CPSCЕ Георгию Маркову (за оригинальные вопросы), а также маркетологу Илье Ануфриеву и корректору Яне Аvezовой (за помощь в оформлении), доцентам и преподавателям кафедры ИУ-8 «Информационная безопасность» МГТУ им. Н. Э. Баумана Виталию Веренице, Игорю Шахалову, Михаилу Никулину, Олегу Гудкову, Сергею Борзых и Анастасии Большаковой (за критику всех зарубежных практик). Авторы также признательны рецензентам учебного курса – профессору Сергею Петренко (СПбГЭТУ «ЛЭТИ») [31] и эксперту SATEC, члену OWASP, GSSP, SCEA, SCJP Alec Shcherbakov (Silicon Value, USA) [67].

Научный редактор
Алексей Марков,
доктор технических наук,
эксперт Российской академии наук

Менеджмент информационной безопасности

В этой главе:

- ◇ *Факторы информационной безопасности*
- ◇ *Система менеджмента информационной безопасности*
- ◇ *Анализ риска*
- ◇ *Классификация информации*
- ◇ *Политики и планы безопасности*
- ◇ *Работа с персоналом*

1.1. Основные понятия информационной безопасности

Под информационной безопасностью (ИБ) системы обычно понимают состояние (свойство) защищенности ее ресурсов в условиях наличия угроз в информационной сфере. С комплексом мероприятий, направленных на обеспечение ИБ, связывают понятие защиты информации.

Определяющими факторами ИБ являются угроза (threat) и риск (risk).

Угрозой называют потенциальную причину (событие, нарушение, инцидент), снижающую уровень ИБ информационной системы, т. е. потенциально способную привести к негативным последствиям и ущербу системы или организации.

Риск представляет собой возможный ущерб, т. е. комбинацию (как правило, произведение), вероятности реализации угрозы и ущерба от нее.

Отметим, что угроза и риск определяются не вообще, а относительно конкретного защищаемого ресурса. В терминологии теории

менеджмента бизнес-процессов вместо ресурса используется синонимическое понятие — актив (asset), под определение которого подпадает все, что имеет ценность для организации, например: базы данных, техническое и программное обеспечение, сетевая инфраструктура, специалисты.

Угрозы ИБ классифицируют по ряду критериев:

- ◇ по причине возникновения (природные или техногенные, в том числе преднамеренные или случайные);
- ◇ по расположению источника (внешние или внутренние);
- ◇ по компрометируемой подсистеме или сегменту (сетевые, криптографические и др.);
- ◇ по этапу формирования в жизненном цикле системы (реализационные и эксплуатационные);
- ◇ по результирующему действию (нарушают уровень конфиденциальности, целостности или доступности).

Примеры угроз ИБ представлены в табл. 1.1.

Таблица 1.1. Примеры угроз информационной безопасности

Задачи обеспечения безопасности	Техногенные		Природные
	Преднамеренные	Случайные	
Контроль физического доступа	Бомбардировка	Сон вахтерши	Торнадо
Сохранность оборудования	Вандализм	Запыление	Шаровые молнии
Управление сетевыми коммуникациями	Прослушивание сети	Флуктуации в сети	Магнитные бури
Защита информационных хранилищ	Взлом парольной системы	Сбой криптосредств	Грибки
Управление непрерывностью деятельности	Последствие DOS-атаки	Последствия тестов на проникновение	Карстовые процессы
Соответствие законодательству	Компьютерное пиратство	Тиражирование персональных данных	Природные пожары

Наиболее известным примером реестра угроз может служить Каталог угроз Федерального агентства по ИБ Германии (BSI IT-Grundschutz-Kataloge)¹.

¹ •RU• В России — Банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru).

Одной из наиболее актуальных угроз ИБ компьютерных систем является возможность реализации уязвимости (vulnerability) системы. Под уязвимостью понимают реализуемый дефект (weakness) технического и программного обеспечения системы, снижающий уровень защищенности ресурсов от тех или иных угроз. Отметим, наличие уязвимости становится угрозой, если ее можно реализовать так, что это приведет к недопустимому ущербу организации. Например, наличие сетевых уязвимостей в программном обеспечении изолированного компьютера не является угрозой.

Известен ряд баз данных уязвимостей, например: OSVDB, Mitre CVE (**Common Vulnerabilities and Exposures**), NVD, CNNVD, JVN iPedia, IBM X-Force и др. Наиболее известной базой описания дефектов безопасности программного кода является реестр Mitre CWE (**Common Weakness Enumeration**).

Умышленная реализация угроз и уязвимостей в компьютерных системах, приводящая к ущербу организации, называется компьютерной атакой («вторжением») на ресурсы. Примером международного каталога шаблонов компьютерных атак является Mitre CAPEC (Common Attack Pattern Enumeration and Classification).

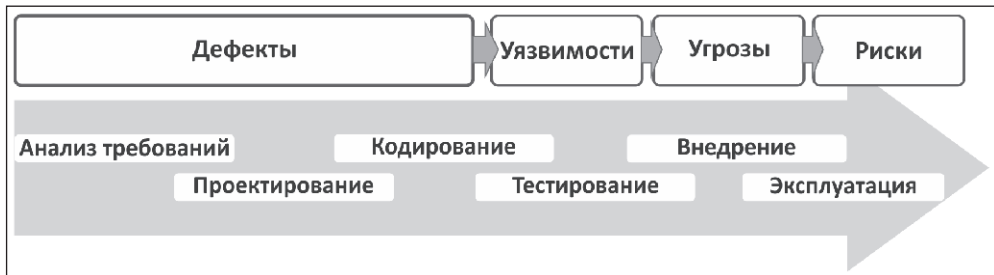


Рис. 1.1. Факторы информационной безопасности в жизненном цикле систем

Понятие ИБ включает в себя совокупность различных свойств, основными из которых являются:

- ◇ конфиденциальность,
- ◇ целостность,
- ◇ доступность.

Конфиденциальность — свойство системы, определяющее ее защищенность от несанкционированного раскрытия информации.

Целостность — свойство, определяющее защищенность от несанкционированного изменения. Разделяют логическую и физическую целостность. Физическая целостность подразумевает неизменность физического состояния данных на машинном носителе. Логическая целостность отражает корректность выполнения вычислительных процессов (транзакций), полноту и непротиворечивость информации, например в СУБД, файловых системах, электронных архивах, хранилищах данных, системах управления документооборотом и т. д.

Доступность — свойство, определяющее возможность за заданное время получить требуемую информационную услугу авторизованному пользователю. С доступностью часто связывают такую характеристику системы, как готовность — способность к выполнению заявленных функций в установленных технических условиях. Атаки, имеющие целью нарушить степень доступности, получили название атак на отказ в обслуживании (DOS-атаки).

Что касается информационной системы, то часто в качестве наиболее важных свойств ее ИБ, для выражения значимости, упоминают свойства аутентичности, подотчетности, неотказуемости, надежности и др.

Повышение и обеспечение заданных уровней конфиденциальности, целостности и доступности ресурсов осуществляются путем применения механизмов ИБ — различных организационно-технических мер ИБ (controls).

1.2. Система менеджмента информационной безопасности

Скоординированные действия, выполняемые с целью повышения и поддержания на требуемом уровне ИБ организации, называются менеджментом (организационно-техническим управлением) ИБ.

Совокупность участников, правил, процедур и мер, используемых для обеспечения требуемого уровня ИБ организации, состав-

ляет систему менеджмента ИБ (СМИБ).

В концептуальном плане СМИБ включает в себя два основных уровня управления:

- ◇ процедурный, касающийся документального оформления бизнес-процессов организации;
- ◇ организационно-технический, касающийся непосредственно мер безопасности.

Процедурный уровень основывается на процессном подходе бизнес-риска, его цель состоит в создании, реализации, эксплуатации, мониторинге, анализе, повышении и поддержке заданного уровня ИБ.

Для практического описания жизненного цикла СМИБ популярна процессная модель PDCA – «Plan (планирование), Do (реализация), Check (проверка) – Act (совершенствование)», известная как цикл Шухарта–Деминга¹. К примеру, на стадии планирования устанавливаются политики ИБ, процедуры, проводится оценка риска. На стадии реализации осуществляются внедрение и поддержка политики ИБ, обработка риска, осуществление контрмер, установка защитных средств и сервисов. На стадии проверки осуществляются контроль факторов ИБ, оценка и анализ эффективности процессов управления ИБ. На завершающей стадии осуществляются выработка и принятие корректирующих и превентивных действий, проводятся переоценка рисков, пересмотр политики и т. д.

При создании СМИБ в первую очередь выбирают наиболее критичные с точки зрения безопасности процессы или процессы, касающиеся определенных видов деятельности организации, например касающиеся международной деятельности или государственного заказа. Соответственно, создание СМИБ может быть поэтапным.

Если обратить внимание на рис. 1.2, можно отметить, что СМИБ не существует сама по себе, а направлена на **удовлетворение** потребностей и ожиданий заинтересованных сторон, как то: руководства организации, клиентов, партнеров, регулирующих органов, сотрудников.

¹ ISO 9001. Quality management systems – Requirements.

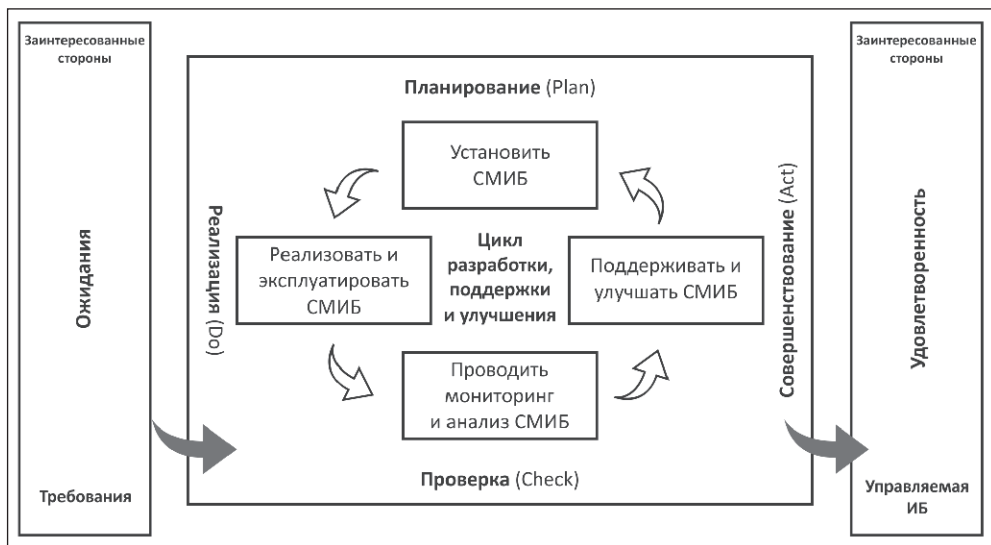


Рис. 1.2. Процессная модель управления информационной безопасностью

Что касается мер, то следует заметить, что в мире¹ сложилась нормативная база менеджмента ИБ, в том числе организационно-технических мер ИБ. Наибольшей популярностью пользуются стандарты ISO 27001 и NIST 800-53 [62]. Например, в ISO 27001:2013 (в приложении А) представлено 114 мер управления и контроля, применяемых в жизненном цикле СМИБ, которые распределены по 14 рубрикам:

- ◇ А.5: Политики информационной безопасности;
- ◇ А.6: Организационные аспекты информационной безопасности;
- ◇ А.7: Вопросы безопасности, связанные с персоналом;
- ◇ А.8: Управление активами;
- ◇ А.9: Управление доступом;
- ◇ А.10: Криптография;

¹ **•RU•** В России, кроме международных стандартов, применяются приказы ФСТЭК России № 17, 21, 31, которые регламентируют национальные организационно-технические (некриптографические) меры обеспечения безопасности информации для некоторых классов информационных систем.

- ◇ А.11: Физическая безопасность и защита от угроз окружающей среды;
- ◇ А.12: Безопасность операций;
- ◇ А.13: Безопасность коммуникаций;
- ◇ А.14: Приемка, разработка и поддержка систем;
- ◇ А.15: Отношения с поставщиками услуг;
- ◇ А.16: Управление инцидентами информационной безопасности;
- ◇ А.17: Аспекты информационной безопасности в обеспечении непрерывности бизнеса;
- ◇ А.18: Соответствие требованиям.

Следует прокомментировать выбор, внедрение и контроль указанных мер ИБ (или «мер управления и контроля»), направленных главным образом на минимизацию остаточных рисков.

В случае внедрения СМИБ в соответствии с ISO 27001:2013 компания руководствуется приложением А стандарта для выбора конкретных мер, при этом исключение меры должно быть обоснованным, как и включение меры, отсутствующей в стандарте. Интересно, что меры неравноценны. В целом меры из приложения А относятся к организационным, например встречаются меры «Политика контроля доступа» (А.9.1.1), «Правила использования активов» (А.8.1.3), предусматривающие определение правил ИБ в форме политик. Что же касается технических мер, то они формулируются общими словами, например: «Безопасность сетевых сервисов» (А.13.1.2).

После решения задачи выбора мер (которые должны быть внедрены, чтобы снизить риски до приемлемого уровня) определяется: что конкретно должно быть сделано, какие ресурсы для этого необходимо задействовать, кто будет ответственным, как будет проводиться оценка выполнения.

На данном этапе разрабатываются политики, процедуры, инструкции (подробнее о них ниже), внедряются технические средства защиты информации, проводится обучение специалистов, задействованных в процессах обеспечения ИБ, внедряется про-

грамма повышения осведомленности сотрудников компании в вопросах безопасности (security awareness program).

В результате внедрения мер должны быть получены работающие процессы СМИБ, которые выполняются, измеряются и контролируются. Необходимо отметить следующие три важные составляющие контроля работы СМИБ:

- ◇ операционный контроль,
- ◇ внутренний аудит,
- ◇ анализ со стороны руководства.

Операционный контроль подразумевает собой текущий контроль со стороны непосредственных руководителей. Например, принятая процедура предусматривает выполнение периодического сканирования на наличие уязвимостей сетевых сервисов, и отвечает за эту функцию конкретный специалист отдела ИБ. Соответственно, руководитель отдела следит за тем, чтобы задача выполнялась подчиненным и чтобы он вовремя получал отчет с результатами сканирования.

Внутренний аудит заключается в периодической проверке эффективности мер. Например, аудитор просит системного администратора предоставить перечень учетных записей, созданных в течение прошлого года, выбирает несколько и просит показать заявки, по которым он может убедиться, что доступ был согласован с руководителями сотрудников и с владельцами системы.

Анализ со стороны руководства подразумевает, что менеджмент интересуется тем, как работает СМИБ, и, в частности, анализирует результаты проведенных аудитов (как внутренних, так и внешних), информацию о количестве произошедших инцидентов ИБ, в каком объеме требуются ресурсы для работы системы и т. п.

Результатом подобных контрольных мероприятий будет информация о недостатках и необходимых улучшениях системы.

Заметим, что в мировой практике, кроме ISO-стандартов, популярностью пользуются представленные в открытом доступе документы NIST [62–66, 70].

Далее в главе мы рассмотрим ключевые аспекты менеджмента ИБ, а именно:

- ◇ риск-ориентированный подход к менеджменту ИБ,
- ◇ классификацию информации и документирование,
- ◇ аспекты человеческого фактора.

1.3. Анализ и управление рисками

1.3.1. Цикл управления рисками

Очевидно, что повышение ИБ не является самоцелью. С точки зрения бизнеса, основная цель реализации тех или иных сервисов ИБ — это всего лишь механизм предотвращения возможного ущерба организации. Основным методом решения задачи *обоснованного* анализа и синтеза мер и средств безопасности является управление рисками (risk management).

Управление рисками представляет собой процесс всестороннего изучения факторов, которые могут привести к реализации возможных угроз по отношению к активам информационной системы, для последующего выбора, реализации и контроля экономически эффективных мер безопасности.

Управление рисками в общем виде включает в себя оценку риска, обработку риска, контроль и оптимизацию рисков.

Процесс оценки рисков включает в себя два этапа:

- ◇ анализ рисков,
- ◇ оценивание рисков.

Анализ рисков имеет целью идентификацию источников и оценку величины риска. В общем виде в анализ риска входят инвентаризация и категорирование ресурсов, идентификация значимых угроз и уязвимостей, а также оценка вероятностей реализации угроз и уязвимостей.

Оценивание риска заключается в вычислении риска и оценивании его по заданной шкале.

Как правило, риск вычисляется как функция от стоимости активов и вероятности реализации тех или иных угроз по отношению к данным активам.

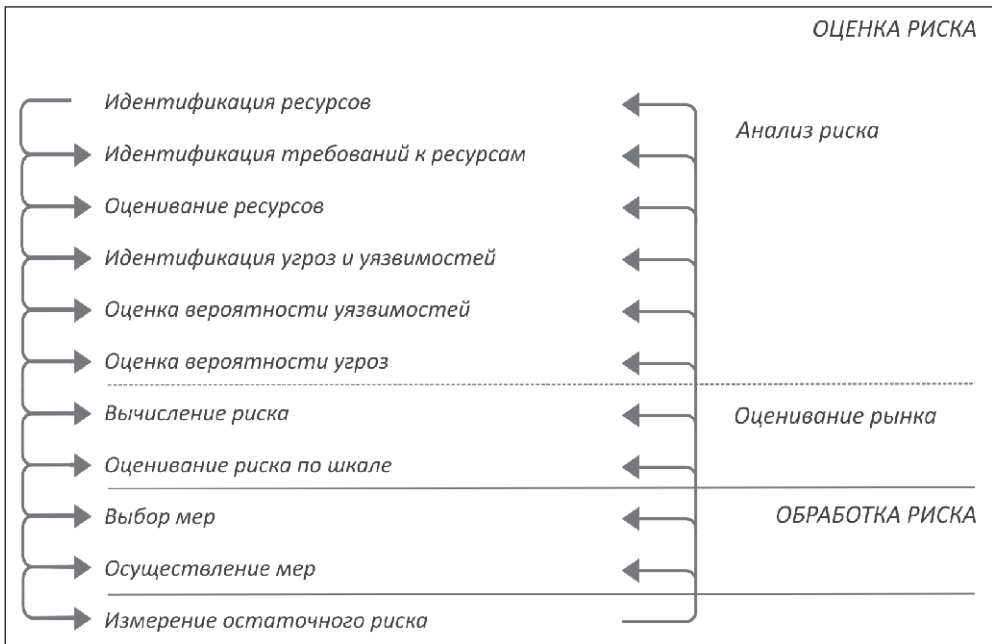


Рис. 1.3. Процедура оценки и обработки риска

После того как риск был оценен, должно быть принято решение относительно обработки этого риска — выбора и реализации мер по модификации риска.

В основу принятия решения кладут ожидаемые потери и частоту возникновения инцидента. Помимо предполагаемых потерь, организация должна также рассмотреть затраты на реализацию решения по обработке риска, а также политику руководства, простоту мер и сервисов безопасности и т. д.

Полученное значение риска анализируется, и выбирается одна из четырех мер обработки риска:

1. Уменьшение риска (*reducing risk, risk mitigation*). Риск считается неприемлемым, и для его уменьшения выбираются и реализуются соответствующие механизмы безопасности.
2. Передача риска (*assigning risk, transferring risk*). Риск считается неприемлемым и на определенных условиях (например, в рамках страхования, поставки или аутсорсинга) переадресуется сторонней организации.

3. Принятие риска (accepting risk). Риск в данном случае считается осознанно допустимым — организация должна смириться с возможными последствиями. Обычно это означает, что стоимость реализации контрмер значительно превосходит финансовые потери в случае реализации угрозы либо организация не может сочинить меры и средства безопасности.
4. Отказ от риска (rejecting risk, ignoring risk). Риск исключается путем отказа от бизнес-процессов организации, являющихся причиной риска. Например, отказ от электронных платежей по Интернету.

В результате обработки риска остается так называемый остаточный риск (residual risk), относительно которого принимается решение о завершении этапа обработки риска.

В результате этого процесса должен быть разработан план обработки рисков.

Международный стандарт ISO 27005 регламентирует общий подход к менеджменту рисков ИБ, а ISO 31010 определяет множество методик и методов анализа риска, как то: «мозговой штурм», структурированные и полуструктурированные опросы, метод Дельфи, контрольные листы, анализ сценариев, ВИА, анализ дерева неисправностей, анализ дерева событий, причинно-следственный анализ, анализ причинно-следственных связей, анализ уровней надежности средств защиты, анализ дерева решений, HRA, анализ диаграммы «галстук-бабочка», цепи Маркова (ТМО), метод Монте-Карло, байесовский подход и сети Байеса, FN-кривые, метод индексов рисков, матрица последствий и вероятностей, многокритериальный анализ решений и др.

Известен ряд технологий и программных средств оценки и управления рисками ИБ, из которых можно назвать: FRAM (Facilitated Risk Analysis Process), CRAMM (CCTA Risk Analysis and Management Method), MSAT (Microsoft Security Assessment Tools), OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) и др.

Ответственность за управление рисками лежит на высшем менеджменте организации (CEO, Chief Executive Officer). В то же

время рутинные операции по оценке, обработке и мониторингу рисков часто делегируются сотрудникам службы ИБ.

1.3.2. Методы оценки рисков

Различают два метода оценки рисков:

- ◇ количественный (quantitative)¹,
- ◇ качественный (qualitative).

Для количественной оценки рисков характерно использование объективных численных, а именно финансовых характеристик. В отличие от количественного, качественный анализ рисков не ставит своей задачей получение численных финансовых характеристик. Для оценки активов и критичности угроз вводится качественная неформальная или полужформальная шкала, и основной целью анализа становится ранжирование угроз в соответствии с выбранными критериями.

В международной практике при проведении количественного анализа часто используются следующие показатели:

- ◇ *EF* – уровень компрометации (Exposure Factor). Данная характеристика определяет, какая часть актива в процентном соотношении будет потеряна в случае реализации угрозы;
- ◇ *SLE* – ожидаемые однократные потери (Single Loss Expectancy). Определяет ожидаемые потери от однократной реализации угрозы и вычисляется по следующей формуле:
$$SLE = AV \cdot EF,$$
где *AV* – стоимость актива;
- ◇ *ARO* – среднегодовая частота реализации (Annualized Rate of Occurrence). Представляет собой ожидаемое количество реализаций угрозы по отношению к активу в течение года;
- ◇ *ALE* – ожидаемые среднегодовые потери (Annualized Loss Expectancy). Определяет ожидаемые финансовые потери от

¹ В ISO 31010 для случая применения шкал используется понятие «полуколичественный» метод.

всех случаев реализации определенной угрозы за год и вычисляется по следующей формуле:

$$ALE = SLE \cdot ARO.$$

Порядок проведения количественной оценки рисков может быть следующим:

- 1) оценка вероятных финансовых потерь путем оценки AV , EF и вычисления SLE ;
- 2) выявление потенциальных угроз и вычисление ARO ;
- 3) вычисление ALE ;
- 4) анализ полученных значений и выбор одной из мер обработки риска, описанных ранее;
- 5) в случае если принято решение о необходимости уменьшения риска, то после выбора механизмов безопасности проводится повторное вычисление ALE с учетом изменившейся вероятности реализации угрозы.

Как правило, на практике точный расчет значений рисков невозможен из-за неопределенности, нечеткости и неточности входных данных, описывающих, по сути, качественные характеристики.

Приведем пример методики качественной оценки уровня рисков:

- 1) с использованием заданных шкал (например, 5-бальных) оцениваются уровни стоимости идентифицированного ресурса и уровни вероятности угрозы;
- 2) по заданной матрице риска (рис. 1.4) рассчитываются уровни риска.

Для определения затрат на обработку рисков может быть выполнено ранжирование инцидентов по уровню риска.

Конец ознакомительного фрагмента.

Приобрести книгу можно

в интернет-магазине

«Электронный универс»

e-Univers.ru