Содержание

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), CPSCE Георгию Маркову (за оригинальные вопросы), а также маркетологу Илье Ануфриеву и корректору Яне Авезовой (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

Глава 1

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–Деминга[1]. К примеру, на стадии планирования устанавливают 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 мире[1] 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:

- ◇ 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;

---

[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.

- ◇ 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.

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» (A.9.1.1), «Правила использования активов» (A.8.1.3), предусматривающие определение правил ИБ в форме политик. Что же касается технических мер, то они формулируются общими словами, например: «Безопасность сетевых сервисов» (A.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.

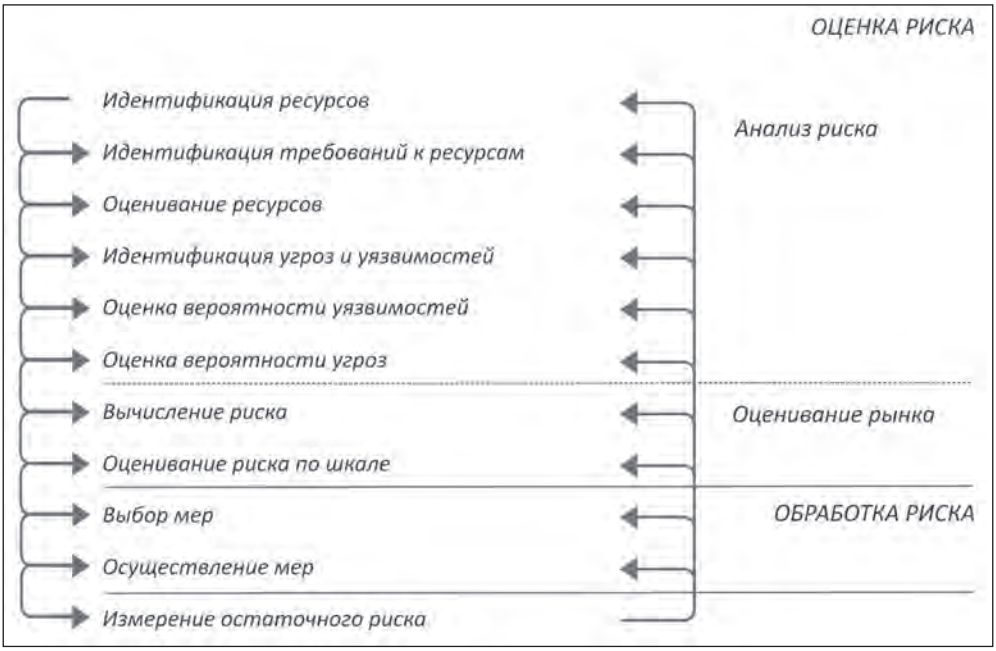

Рис. 1.3. Процедура оценки и обработки риска

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 отработки 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, BIA, 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 (TMO), 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 полуформальная 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.

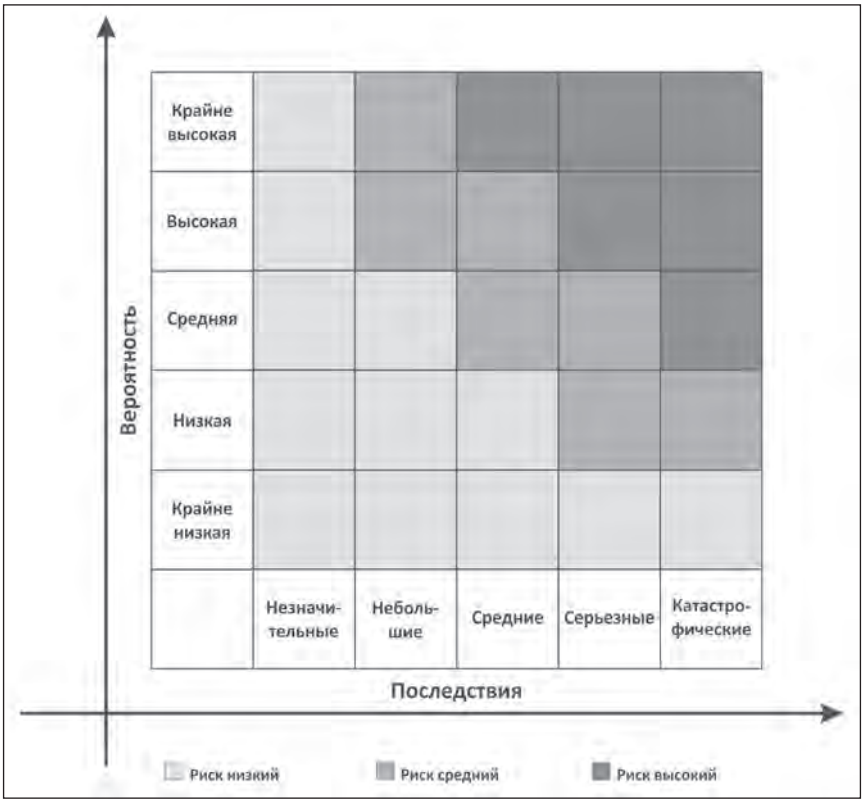

Рис. 1.4. Матрица оценки рисков

1.3.3. Выбор мер безопасности

При минимизации риска главным критерием выбора мер и средств безопасности является экономическая эффективность, которая обычно количественно оценивается с помощью показателя *ROI* (Return on Investment — отдача от инвестиций):

$$ROI = NVP\,(\Delta ALE - AT),$$

где AT — годовые затраты на внедрение и поддержку механизма безопасности, ΔALE — ожидаемое снижение среднегодовых потерь от внедрения механизма безопасности, NPV — коэффициент инфляции (Net Present Value).

Данный показатель позволяет наглядно оценить выигрыш (или отсутствие такового) от использования того или иного механизма безопасности.

Другими важными факторами, влияющими на выбор мер безопасности, являются отраслевые стандарты и правовые нормы, которые в ряде случаев требуют использования детерминированных технологий и механизмов безопасности, возможно, не являющихся оптимальными с экономической точки зрения. Примером может служить требование по использованию ведомственных сертифицированных средств защиты информации для систем, обрабатывающих информацию, составляющую государственную тайну, или персональные данные.

1.4. Классификация информации

При управлении ресурсами самыми важными являются их классификация и определение ответственности за них. Дело в том, что в информационных системах обрабатывается и хранится, как правило, информация разного уровня значимости с точки зрения ИБ. Например, в системе может быть информация как открытая (общедоступная), так и ограниченного доступа. Кроме того, к различным наборам и потокам данных могут предъявляться различные требования по доступности и целостности, а также и другие требования, определяемые спецификой бизнес-процессов организации.

Для обоснования необходимого уровня защиты информации предназначена процедура классификации (категорирования) информации (information classification) — распределение информации по различным классам ИБ. Результаты классификации позволяют структурировать документооборот, определить критические подсистемы, сформировать требования и выбрать меры и сервисы безопасности.

Исторически категорирование информации возникло как элемент обеспечения ИБ в национальных и оборонных информационных инфраструктурах. В большинстве развитых стран сложилась градация информации на относящуюся и не относящуюся к госу-

дарственной тайне – а последняя, в свою очередь, классифицируется по степени секретности[1]. Например, в ряде стран можно встретить следующую классификацию информации:

- ◇ Top Secret – информация, которая имеет важное значение для обеспечения национальной безопасности;
- ◇ Secret – информация, разглашение которой может причинить серьезный ущерб национальным интересам;
- ◇ Confidential – информация, разглашение которой может причинить ущерб национальным интересам;
- ◇ Sensitive (Controlled, Restricted, For Official Use Only, Limited Distribution) Unclassified Information – информация, не являющаяся общедоступной, однако не способная причинить значительного ущерба национальным интересам в случае ее разглашения;
- ◇ Unclassified – общедоступная информация.

В ряде зарубежных стран ограничения к информации вводятся дополнительно политиками по безопасности разного типа объектов информатизации.

Для получения доступа к какой-либо из классифицированной информации должны быть выполнены два условия:

- ◇ пользователь должен иметь соответствующий уровень допуска (clearance);
- ◇ соответствующая информация должна иметь непосредственное отношение к деятельности пользователя.

Последнее требование очень важно, т. к. реализует так называемый принцип «**положено знать** только то, что связано с профессиональной необходимостью» (need-to-know). Для этого в пределах одного уровня секретности производится дополнительное

---

[1] **•RU•** В России информация ограниченного доступа разделяется на составляющую государственную тайну («особой важности», «совершенно секретно», «секретно») и информацию ограниченного доступа, не относящуюся к государственной тайне (конфиденциальная информация). К конфиденциальной информации относят около полусотни видов тайн: коммерческую тайну, врачебную тайну, личную и семейную тайну (персональные данные) и др.

разграничение доступа к информации по смысловым категориям[1]. К примеру, пусть пользователь имеет допуск к информации с грифом «особой важности». В таком случае это совершенно не означает наличия его доступа к любой информации данной степени секретности. Пользователь может получить только ту информацию, которая имеет непосредственное отношение к его служебной деятельности.

С учетом вышеизложенного идею классификации информации можно представить рис. 1.5.

Рис. 1.5. Уровни классификации информации

Для негосударственных структур выбор уровней конфиденциальности и категорий защищаемой информации может быть выполнен произвольно с учетом специфики конкретной организации.

На практике при проведении классификации информации в качестве критериев могут быть определены следующие:

1) ценность информации (value). Это наиболее универсальный критерий классификации информации, допускающий очень широкое толкование. Обычно ценность легко выражает-

[1] Например, гриф секретности может быть помечен дополнительной литерой.

ся в денежных единицах (например, можно количественно оценить стоимость уникальной продукции). Иногда ценность определяется качественно (например, трудно оценить материальный ущерб от незапланированного раскрытия финансовых показателей компании, однако потери могут быть вполне ощутимыми);

2) возраст информации (age). Во многих случаях актуальность (и, соответственно, ценность) информации уменьшается с течением времени;

3) юридические аспекты. Определенные категории информации в соответствии с законодательством большинства стран подлежат защите в обязательном порядке. Это прежде всего государственная тайна, персональные данные (приватная информация о сотрудниках), данные по налогообложению, врачебная тайна и т. п.

Приведем типовой порядок классификации информации.

Первое — это назначение сотрудника, ответственного за классификацию информации. Данная роль является одной из самых критичных для всей системы обеспечения ИБ организации.

Второе — следует выбрать критерии для классификации информации. Выбор одного или нескольких из приведенных выше критериев должен быть обусловлен спецификой организации. Первичную классификацию осуществляет владелец информации, однако результаты контролируются вышестоящим руководителем.

Далее следует провести идентификацию и документирование всех исключений из общих правил, существующих в системе классификации информации.

После этого осуществляются выбор и документирование сервисов безопасности, применяемых для защиты информации каждого из уровней конфиденциальности.

Затем выполняются определение и документирование порядка изменения уровня конфиденциальности для тех или иных данных. Данная процедура может потребоваться, например, в случае возникновения необходимости передачи категорированных данных за пределы автоматизированной системы организации.

В завершение следует организовать доведение до сотрудников компании порядка обращения с классификационной информацией. Данный аспект является одним из важнейших, поскольку адекватная реализация многоуровневой политики безопасности принципиально невозможна в случае непонимания сотрудниками ее базовых принципов.

Отдельного рассмотрения заслуживает порядок изменения уровня конфиденциальности информации. Отметим, что, кроме истечения заданного срока конфиденциальности информации, поводом для ее раскрытия может стать, например, судебный запрос.

Важно заметить, что классифицированная информация должна подлежать **маркированию**, т. е. указанные данные должны содержать соответствующую метку или гриф (представленные в физическом или, если последнее невозможно, в электронном формате).

В рамках данной темы следует определить участников классификации информации:

1. **Владелец** информации (owner, stakeholder). Владелец информации определяется для каждого защищаемого ресурса. Часто владельцем выступает менеджер высшего уровня. Владелец несет полную личную ответственность (это определено в законодательстве ряда стран) за указанный ресурс, в том числе за выбор мер и сервисов безопасности. Владелец выполняет следующие функции:
   - ◇ определяет классификацию информации;
   - ◇ периодически пересматривает уровень классификации информации с учетом произошедших изменений;
   - ◇ делегирует выполнение определенных операций, связанных с внедрением мер и сервисов безопасности (но ответственность несет сам) администратору.
2. **Администратор** данных (custodian, trustee). Администратор получает определенные полномочия по обеспечению защиты категорированной информации от владельца, например выполнение сервисных операций по резервному копированию и восстановлению.

3. **Пользователь** (user). Под пользователем в данном случае понимается сотрудник, использующий категорированную информацию для выполнения своих обязанностей. При этом:
   - ◇ пользователи должны следовать инструкциям, полностью соответствующим политике безопасности организации;
   - ◇ необходимо обеспечить возможность доступа пользователей исключительно к тем информационным ресурсам, которые имеют непосредственное отношение к функциональным обязанностям;
   - ◇ необходимо обеспечить, чтобы пользователи обращались к ресурсам корпоративной автоматизированной системы исключительно для служебных, а не для персональных целей.
4. **Аудитор** (auditor) — специалист, на которого возложены функции объективного контроля.

Следует заметить, что в международной практике общие обязанности участников связаны с этическими принципами, в частности: «должная забота» (due care) и «должная осмотрительность» (due diligence), в которых делается акцент на всесторонней обоснованности решений в зависимости от реальных обстоятельств, ну и на здравом смысле.

1.5. Порядок использования политик, стандартов и руководств

Очевидно, что «спонтанно бессознательная» организация управления неприменима для сложных систем, поэтому СМИБ основывается на наборе внутренних нормативных документов: политиках, процедурах, корпоративных стандартах, руководствах и инструкциях.

Политика (policy) представляет собой документ, в котором определяются цели, задачи и пути их достижения, принципы.

Следует помнить, что часто под политикой информационной безопасности (information security policy) понимается высокоуровневый документ (одобренный руководством организации), предна-

значенный для обеспечения управления ИБ в соответствии с требованиями бизнеса, партнеров, клиентов, законодательной базы.

Высокоуровневая политика безопасности, как правило, представляет собой достаточно статичный документ. Такой документ обычно содержит:

- ◇ общую информацию об обеспечении ИБ в организации (в которой мотивированно определена необходимость обеспечения и поддержки режима безопасности);
- ◇ заявление о поддержке (commitment) мероприятий по обеспечению ИБ на всех управленческих уровнях;
- ◇ основные положения по определению целей ИБ;
- ◇ распределение ролей и определение общей ответственности за реализацию мероприятий по обеспечению ИБ (в том числе по разработке и корректировке политик);
- ◇ основные положения по определению целей и механизмов безопасности, включая структуру оценки и управления рисками (допустимый риск, например);
- ◇ ссылки на низкоуровневые документы, конкретно определяющие порядок реализации тех или иных аспектов, связанных с обеспечением ИБ.

Документированная политика ИБ должна быть утверждена руководством организации и доведена до сведения всех сотрудников организации и внешних сторон, к которым она относится.

Кроме высокоуровневой политики, выделяют низкоуровневые политики (частные политики), как правило, отражающие требования в определенной области или сегменте. В качестве примеров политик низкого уровня можно привести политику управления доступом, политику управления паролями, политику резервного копирования, политику по защите интеллектуальной собственности и т. п.

Состав частных политик зависит от особенностей организации: ее размера, структуры, корпоративной культуры и т. п.

На нижележащем уровне иерархии документов, регламентирующих процесс обеспечения ИБ в организации, находятся стандарты организации, руководства и инструкции.

Корпоративные стандарты или нормы (standard) определяют обязательное требование, практику применения какого-либо решения. Примером корпоративного стандарта является, например, стандарт на конфигурацию серверов под управлением определенной операционной системы.

Руководства (guidelines) отличаются от стандартов в первую очередь тем, что носят рекомендательный характер. Руководства, в частности, могут определять, как именно следует реализовывать то или иное требование на практике с учетом локальной специфики. Так, например, специалист по информационной безопасности может разработать руководство, описывающее различные алгоритмы генерации надежных паролей, чтобы облегчить задачу выбора пароля пользователю.

Инструкции или процедуры (procedure) представляют собой документ, определяющий последовательность действий по выполнению какой-либо задачи в соответствии с требованиями политик и стандартов. Из процедуры должно быть ясно, кто, что и когда делает. Хорошим примером процедуры является процедура регистрации пользователей в системе, описывающая этапы согласования заявки на доступ.

Необходимо отметить, что в основном упомянутые документы ориентированы на специалистов отделов ИТ/ИБ, руководителей подразделений. Для неподготовленных сотрудников содержание данных документов может быть непонятным. В таких случаях разрабатывается документ «Свод правил для сотрудников», в котором доступным языком без использования технических терминов формулируются требования, которые должны выполнять сотрудники. Также функциональные возможности по обеспечению ИБ должны быть закреплены в положениях об отделах и должностных инструкциях.

К отдельным видам документов стоит отнести так называемые записи (records). Записи представляют собой те документы, которые создаются при выполнении процедуры, например заявка на предоставление доступа к системе, журнал системы контроля доступа с информацией о том, кто входил в серверное помещение, и т. п.

При внедрении СМИБ названия документов и их состав определяют, исходя из устоявшейся практики в компании. Политика может называться концепцией или положением, процесс — порядком и т. п.

На рис. 1.6 представлен возможный вариант структуры документации СМИБ.

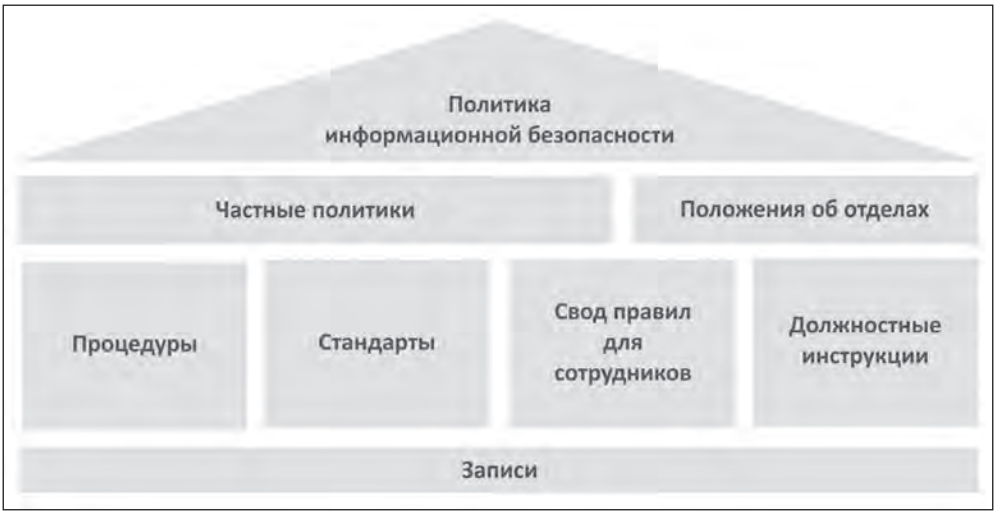

Рис. 1.6. Возможная структура документации СМИБ

1.6. Особенности работы с персоналом

Человеческий фактор является наиболее уязвимым звеном любой информационной системы, поэтому меры по работе с персоналом являются важнейшим компонентом СМИБ. Структура организации может накладывать свою специфику на используемые методы, однако в общем случае необходимо предусмотреть следующие механизмы:

1) документальное закрепление роли и обязанности каждого сотрудника (в соответствии с политикой безопасности). Особо должны быть выделены меры, которые предпринимаются в случае, если сотрудник игнорирует требования безопасности организации;

2) проверка при трудоустройстве. В зависимости от критичности предполагаемой должности нового сотрудника проверка может включать подтверждение данных, представленных в резюме, просмотр кредитной истории, контроль наличия криминальных связей и сомнительного прошлого;
3) включение аспектов, связанных с поддержанием режима обеспечения ИБ, в трудовой договор. В обязательном порядке в договор должны быть включены вопросы, связанные с ограничением приватности: согласие сотрудника на мониторинг электронной почты, прослушивание телефонных переговоров;
4) как правило, в виде самостоятельного документа сотрудник подписывает **договор о конфиденциальности и неразглашении** (non-disclosure agreement, NDA). Данная мера позволяет избежать распространения конфиденциальной корпоративной информации уволившимися сотрудниками;
5) внутренние системы допусков к конфиденциальной информации. Получению допуска должны предшествовать комплексные проверки, направленные на выявление возможной неблагонадежности сотрудника. Согласие на такие проверки может быть также отражено в трудовом договоре;
6) в целях борьбы с мошенничеством и для критических бизнес-процессов могут быть предусмотрены особые процедуры, предусматривающие разграничение обязанностей (например, выполнение финансовой операции и контроль ее правильности), а также ротацию;
7) система обучения сотрудников. Вопросы обеспечения ИБ и соответствующие организационные и технические меры не являются очевидными для большинства сотрудников. Учебные курсы, семинары, справочные буклеты и другие подобные механизмы, направленные на разъяснение принципов и правил защиты информации, позволяют значительно повысить эффективность используемых средств защиты;
8) корректное увольнение сотрудников. Процедура увольнения может сопровождаться всплеском негативных эмоций, что

не должно привести к реализации тех или иных угроз ИБ. Во избежание злонамеренных действий со стороны уволенного сотрудника необходимо предусмотреть такие механизмы, как немедленное блокирование (но не удаление) учетной записи, закрытие физического доступа в помещение компании, сопровождение увольняемого сотрудника офицером службы безопасности. Разумеется, важно корректно организовать возврат ресурсов, которые были в его пользовании.

Вопросы для повторения

1. Укажите, что относится к основным свойствам информационной безопасности:
   a) риски, угрозы, уязвимости, дефекты;
   b) «конфиденциально», «секретно», «совершенно секретно», «особой важности»;
   c) конфиденциальность, аутентичность, подотчетность, неотказуемость и надежность;
   d) доступность и конфиденциальность, а также целостность.

2. Какое определение наиболее корректно по отношению к понятию риска ИБ:
   a) риск — вероятность несанкционированного доступа к информации;
   b) риск — вероятность события, которое может привести к нарушению уровня ИБ (нарушениям конфиденциальности, целостности, доступности ресурса);
   c) риск — особенность характера нарушителя;
   в) риск — произведение значений вероятности события и квадрата его последствий для ИБ.

3. Какая схема на рис. 1.7 правильно описывает процессный подход к управлению ИБ:

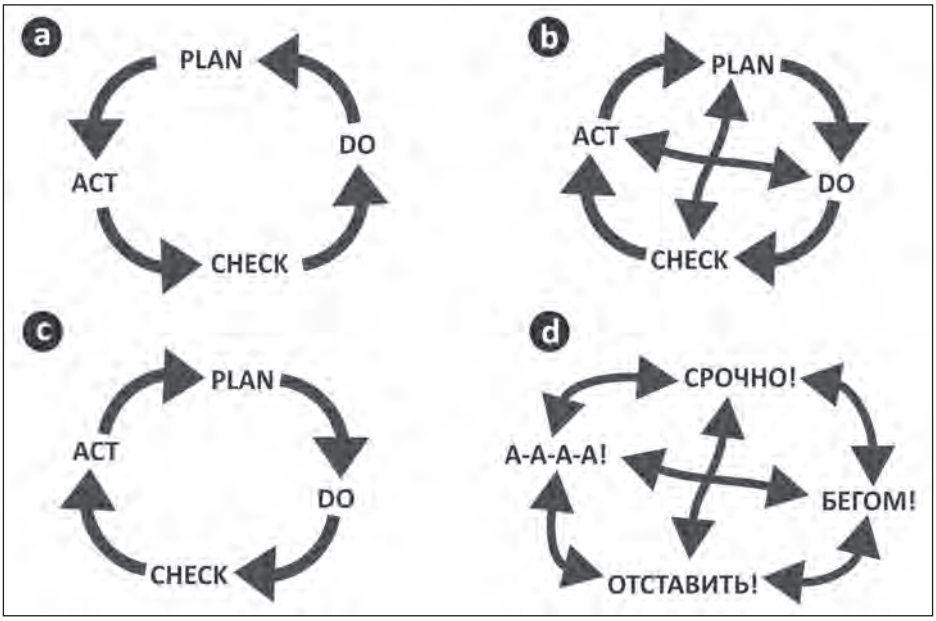

Рис. 1.7. Возможные процессные модели

4. Какой из перечисленных ниже способов управления рисками является наиболее нежелательным:
   a) принятие риска;
   b) уменьшение риска;
   c) передача риска;
   d) отказ от риска.

5. Укажите, кто определяет первичный уровень конфиденциальности информации:
   a) администратор безопасности;
   b) собственник системы;
   c) владелец информации;
   d) руководитель организации.

6. Отметьте, что, как правило, не относят к активам ИБ:
   a) деньги;
   b) инфраструктуру;
   c) сотрудниц;
   d) информационное обеспечение.

7. Что означает принцип «положено знать» (need-to-know):
   a) пользователь информации должен знать об ответственности в случае нарушения им правил доступа к информации;
   b) владелец информации должен знать, кто имел доступ к его информации;
   c) в пределах одного уровня секретности производится дополнительное разграничение доступа к информации по смысловым категориям;
   d) пользователь, имеющий доступ к информации заданного уровня секретности, должен иметь доступ и к информации низшего уровня секретности.

8. Что делать, если в компании не хватает финансовых средств на исключение всех уязвимостей:
   a) предложить руководству изыскать дополнительные средства, объяснив уголовную ответственность руководства и обосновав окупаемость контрмер;
   b) сосредоточиться на наиболее критичных уязвимостях;
   c) уделить внимание всем уязвимостям в равной степени, чтобы каждая уязвимость могла иметь хоть какую-нибудь защиту;
   d) используя принцип «скрытия данных по ИБ», постараться замолчать указанную проблему до лучших времен.

9. Оборудование инновационного технопарка оценивается в 1 000 000€. Согласно заявлению материально-технической службы, два раза в неделю фиксируется факт пропажи. По оценкам экспертов, недобропорядочный сотрудник в случае удачи способен вынести до 0,1% оборудования. Выберите максимальное значение ALE:
   a) 10;
   b) 285;
   c) 28 500;
   d) 104 000.

10. Стоимость оборудования космической связи между сибирскими поместьями составляет 5000$. Согласно статистике, заблуд-

шие медведи царапают фотонные отражатели антенн два раза за летний сезон. Несмотря на то что инженеры подручными средствами легко обеспечивают работоспособность оборудования, им за раз требуется на протирку микросхем пол-литра технического спирта по цене 1$ за литр. Оцените ALE:

a) 10002;
b) 2500;
c) 1;
d) 0,25.

11. Какие документы по ИБ имеют обязательный характер в организации:

a) профили защиты;
b) рекомендательные письма от известных родителей;
c) руководящие указания;
d) стандарты организации.

12. Что имеет первостепенное значение при организации системы защиты:

a) выбор эффективных средств скрытого наблюдения;
b) информирование и организация эффективного обучения;
c) одобрение руководством;
d) разработка ценных указаний.

Лабораторная работа

Задача: используя стандарт ISO 27001:2013 (приложение A), выбрать меры (controls), которые были нарушены, и заполнить отчет о несоответствии (рис. 1.8).

Исходные данные:

1. Принятая в компании процедура требует, чтобы ПО устанавливалось после согласования с IT-менеджером.
2. Во время аудита было обнаружено, что в отделе маркетинга один сотрудник самостоятельно установил ПО, а руководитель отдела маркетинга не обратил на это внимания.

Внутренний аудит СМИБ			
Отчет о несоответствии			
Департамент:	*Маркетинг*	Дата аудита:	*дд.мм.гг*
Владелец процесса:		Аудитор:	
Номер несоответствия:			
Требование *(из приложения А)*	Обнаружение		
A.?.?.? *A.?.?.?*			
Владелец	Действия по исправлению ситуации		
Руководитель департамента маркетинга	- - -		
Аудитор	Последующая проверка		
ФИО	- -		

Рис. 1.8. Шаблон отчета о несоответствии