Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 9 (76)/1999

Аудит безопасности информационных систем

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Аудит безопасности информационных систем

Сергей Симонов

СОДЕРЖАНИЕ

1. Введение

Обеспечение информационной безопасности (ИБ) компьютерных систем различного назначения продолжает оставаться чрезвычайно острой проблемой. Можно констатировать, что несмотря на усилия многочисленных организаций, занимающихся решением этой проблемы, общая тенденция остается негативной. На рис. 1 представлен прогноз роста числа инцидентов в области ИБ, имеющих тяжелые последствия в крупных организациях по данным [1]. Основных причин две:

- Возрастающая роль информационных технологий в поддержке бизнес-процессов, как следствие возрастающие требования к ИБ автоматизированных систем. Цена ошибок и сбоев информационных систем возрастает.
- Возрастающая сложность информационных процессов. Это предъявляет повышенные требования к квалификации персонала, ответственного за обеспечение ИБ. Выбор адекватных решений, обеспечивающих приемлемый уровень ИБ при допустимом уровне затрат, становится все более сложной задачей.

Первая причина носит объективный характер, ей можно противопоставить только способность организации обеспечивать возрастающие требования в области ИБ.

Рис. 1. Прогноз роста числа инцидентов в области ИБ, имеющих тяжелые последствия.

Для нейтрализации воздействия второй причины необходимо отслеживать соответствие квалификации персонала, ответственного за обеспечение ИБ и стоящих задач, получить объективную оценку состояния подсистемы ИБ.

Для решения этих задач создаются организации аудиторов в области ИБ, ставящие своей целью проведение экспертизы соответствия системы ИБ некоторым требованиям, оценки системы управления ИБ, повышения квалификации специалистов в области ИБ. Статус таких организаций может быть как государственный (при национальных институтах стандартов) так и независимых международных организаций.

Идея проведения аудита ИБ и аттестации информационной системы на соответствие некоторым требованиям не нова. Система аттестации обычно появляется одновременно с принятием стандартов ИБ.

В последнее время в разных странах появилось новое поколение стандартов в области ИБ, посвященных практическим аспектам организации и управления ИБ, некоторые рассмотрены в [2]. Особого внимания заслуживает британский стандарт BS7799 и ассоциированные документы, как наиболее проработанные и апробированные.

Построение системы управления ИБ в соответствии с этими стандартами предполагает наличие (см. рис. 2):

- явно декларированных целей в области безопасности;
- эффективной системы менеджмента ИБ, имеющей совокупность показателей для оценки ИБ в соответствии с декларированными целями, инструментарий для обеспечения ИБ и оценки текущего ее состояния;
- некоторой методики проведения аудита ИБ, позволяющей объективно оценить положение дел в области ИБ.

Технология проведения аудита на соответствие подобным стандартам существенно отличается от технологий, применяемых для предыдущих поколений стандартов, к которым, в частности, относятся Руководящие документы (РД) Гостехкомиссии России 1992 – 1993 гг. Основное отличие заклю-

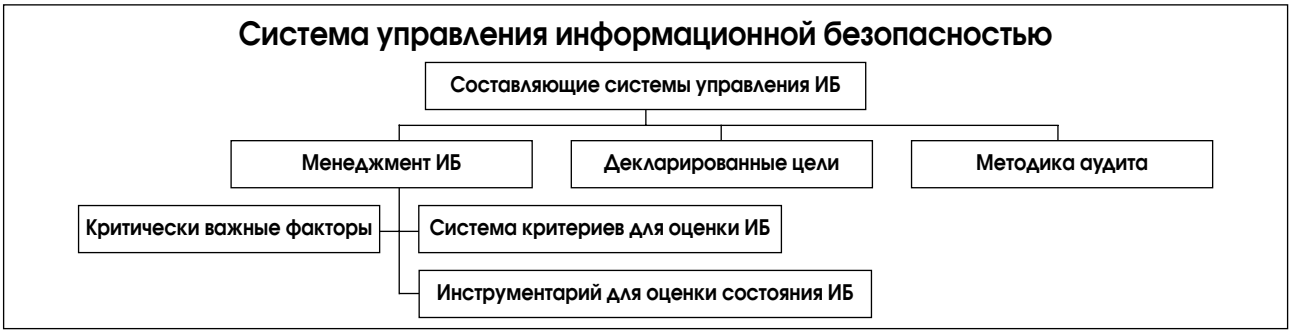

Рис. 2. Построение системы управления ИБ в соответствии с национальными и международными стандартами.

чается в гораздо большей степени формализации некоторых этапов, использовании поддающихся проверке показателей и критериев, то есть в большей детализации. Это, конечно, эволюционный путь развития, но на него в настоящее время специалистами возлагаются большие надежды: считается, что именно широкое использование процедур добровольной сертификации позволит переломить негативную тенденцию возрастания числа инцидентов в области ИБ, имеющих тяжелые последствия.

Следует отметить, что должный эффект может дать только комплексный подход к аудиту, то есть проверка на соответствие определенным требованиям не только программно-технической составляющей некоторой информационной технологии, но и решений на процедурном уровне (организация работы персонала и регламентация его действий) и административном уровне (корректность существующей программы обеспечения ИБ и практика ее выполнения). Иллюстрацией этого положения являются рис. 3-5, построенные на основании данных Института компьютерной безопасности (Computer Security Institute, CSI).

Ниже рассматриваются особенности современных зарубежных стандартов в области аудита и сертификации, введенных в действие в 1998 г, а также действующие в настоящее время Российские руководящие документы в области сертификации и аттестации.

2. Зарубежные подходы к аудиту и сертификации

2.1. Аудиторы в ожидании бума сертификации подсистем ИБ

Некоторые специалисты [1] предсказывают наступление в скором времени бума добровольной сертификации, полагая, что это позволит резко улучшить положение в области ИБ работающих систем.

Основанием для такого вывода являются данные, представленные на рис. 6. Британский стандарт со спецификациями системы управления ИБ [4], являющийся основой для проведения аудита ИБ, вышел в 1998 году, рис. 6 отражает положение дел в 1999 году (по данным Британского института стандартов (BSI)). Всего за год существования стандарта и, соответственно, начала действия системы сертификации на его основе, около 3% фирм уже прошли сертификацию, около трети имеют твердые планы сделать это в ближайшее время и находятся на различных стадиях подготовки к сертификации. Более трети собирает дополнительную информацию, рассматривает такую возможность. Сознательно не собираются проводить сертификацию только 21% фирм.

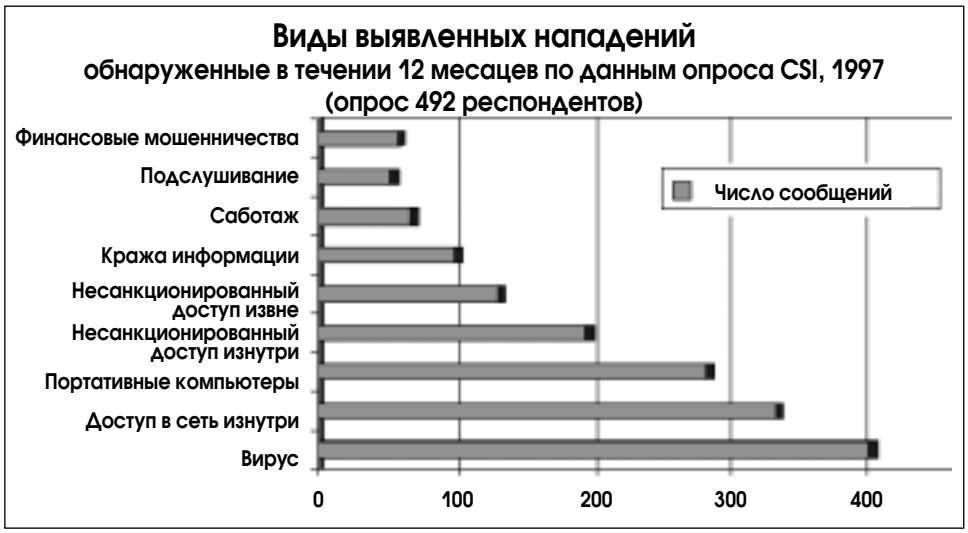

Рис. 3. Виды выявленных нападений.

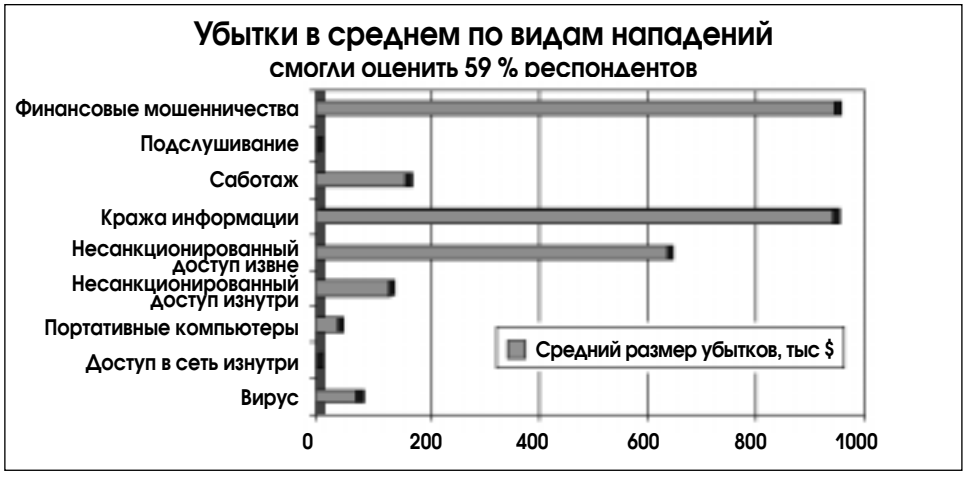

Рис. 4. Ущерб по видам нападений.

Основной причиной добровольной сертификации является желание повысить уровень ИБ, то есть большинство руководителей уверено в действенности подобного мероприятия.

Следует отметить, что приведенные цифры отражают положение дел в Великобритании. В этой стране имеется длительный опыт (с 1993 года) добровольного применения стандарта по управлению информационной безопасностью [3], который в настоящее время применяет более 60 % организаций. Добровольная

сертификация на соответствие этим стандартам — логичное продолжение установившейся практики.

В других странах желающих пройти добровольную сертификацию меньше, но тенденция та же: независимый аудит ИБ начинают рассматривать как весьма действенное средство обеспечения режима ИБ. Кроме национальных институтов стандартов, работы по выполнению аудита выполняет ряд независимых международных организаций, например, Ассоциация аудита и управления информационными системами (The Information Systems Audit and Control Association & Foundation — ISACA).

Ниже рассматриваются основные особенности проведения аудита в соответствии с Британским стандартом [4] и стандартами ассоциации аудита и управления информационными системами [5].

2.2. Британская система сертификации

Основные положения британских стандартов BS7799 «Практические рекомендации по управлению информационной безопасностью» излагались ранее [2]. Рассмотрим процедуру проведения аудита информационных систем в соответствии с этим стандартом.

Вопросы сертификации в Великобритании курирует BSI, под его контролем служба UKAS — United Kingdom Accredited Service занимается аккредитацией организаций на право аудита ИБ в соответствии со стандартом BS7799. Сертификаты, выданные этими органами, признаются не только в Великобритании, но и во многих других странах.

Организация, решившая провести аудит ИБ, должна провести подготовительные мероприятия, привести в соответствие с требованиями стандарта документацию и систему управления ИБ. После этого приглашается аудитор. Процедура аудита рассматривается ниже, ее трудоемкость для крупных организаций может достигать 25-30 человеко-дней работы аудитора. Сертификаты выдаются после проведения аудита подсистемы ИБ на соответствие стандартам BS7799 и действительны в течение 3 лет.

2.2.1. Подготовка организации к аудиту

Подготовительные мероприятия включают подготовку документации и проведение внутренней проверки соответствия системы управления ИБ требованиям стандарта. Документация должна содержать:

- политику безопасности;
- границы защищаемой системы;
- оценки рисков;
- управление рисками;
- описание инструментария управления ИБ;
- ведомость соответствия — документ, в котором оценивается соответствие требованиям стандартов поставленных целей в области ИБ и средств управления ИБ.

Внутренняя проверка соответствия системы управления ИБ требованиям стандарта состоит в проверке выполнения каждого положения стандарта. Проверяющие должны ответить на два вопроса: выполняется ли данное требование, и если нет, то каковы точные причины невыполнения?

На основе ответов составляется ведомость соответствия. Основная цель этого документа — дать аргументированное обоснование имеющим место отклонениям от требований стандарта.

После завершения внутренней проверки устраняются выявленные несоответствия, которые организация сочтет нужным устранить.

2.2.2. Аудит подсистемы ИБ на соответствие стандартам BS7799

Аудиторы должны проанализировать все существенные аспекты с учетом размера проверяемой организации и специфики ее деятельности,

Рис. 5. Субъективная оценка вероятных источников нападений.

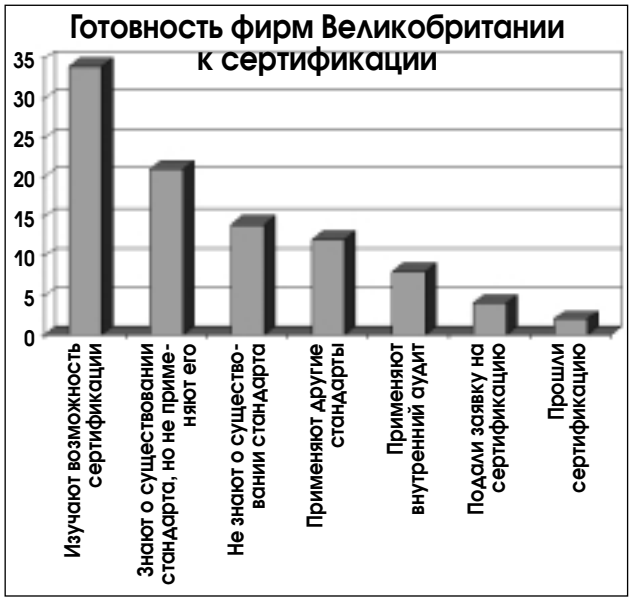

Рис. 6. Готовность фирм Великобритании к сертификации.

а также ценности информации, подлежащей защите. Как следствие, опыт и компетентность аудитора являются очень существенными факторами.

Задачи аудита (сертификации)

В результате проведения аудита создается список замечаний, выявленных несоответствий требованиям стандартов, а также рекомендаций по их исправлению. Аудиторы должны гарантировать, что были выполнены все требования процедуры сертификации.

Категории несоответствий

И аудиторам, и проверяемой организации необходимо иметь четкое представление о степени серьезности обнаруженных недостатков, их категориях и способах исправления. Используются следующие категории несоответствия:

- **Существенное несоответствие**. Не выполняется одно или несколько базовых требований стандартов, либо установлено, что используются неадекватные меры по защите конфиденциальности, целостности или доступности критически важной информации.
- **Несущественное несоответствие**. Не выполняются некоторые второстепенные требования, что несколько повышает риски или снижает эффективность защитных мер.

Каждое несоответствие должно иметь ссылку на соответствующее требование стандартов.

В случае, если выявлено значительное количество несущественных несоответствий, аудитор должен рассмотреть вопрос о возможном появлении существенного несоответствия.

После выявления несоответствий аудитор и представители организации должны наметить пути их устранения.

Если аудитор считает, что подсистему ИБ возможно усовершенствовать, то он может составить замечание. Организации сами определяют, какие действия им следует предпринять в ответ на замечание. Замечания фиксируются, и при последующих проверках аудиторы должны выяснить, что было сделано.

Организация аудита

Подготовка и планирование аудита

Процедура проведения аудита планируется заранее. План проведения аудита должен быть подготовлен для всех первоначальных и контрольных проверок, продолжающихся более одного дня. Аудиторы должны быть ознакомлены с законодательными и нормативными требованиями, используемыми в проверяемой организации.

Проверка документации

Сертификация начинается с того, что аудитор получает и анализирует документы, имеющие отношение к подсистеме ИБ. Организация должна представить следующие документы:

- концепцию политики ИБ, границы подсистемы ИБ, документы по оценке рисков;
- руководство по реализации политики безопасности, содержащее общую схему подсистемы ИБ и документированные процедуры обеспечения ИБ;
- ведомость соответствия — документ, составленный аудитором при предыдущей проверке. Содержание этого документа будет рассмотрено ниже.

По окончании проверки представляется отчет, в котором должны быть отражены следующие моменты:

- декларируемые цели в области ИБ достижимы (являются реалистичными);
- ведомость соответствия не противоречит стандартам в области ИБ и политике безопасности;
- должным ли образом описаны все соответствующие аспекты в процедурах обеспечения ИБ.

Подготовительный этап – планирование проведения аудита

План проведения аудита должен определять подлежащие проверке сферы деятельности организации. В плане должно быть указано, какие требования стандарта будут проверяться (согласно Ведомости соответствия). Этот план, вместе со всеми изменениями, внесенными в процессе выполнения аудита, прилагается к отчету о проведении аудита.

План составляется на основе следующих документов:

- Руководство по реализации политики безопасности;
- Ведомость соответствия.

Организация должна представить сведения о собственной структуре, текущей деятельности, проектах и т.д. Кроме того, потребуется описание используемых информационных технологий, включающее схему сети, а также список всего прикладного программного обеспечения, используемого в организации.

Совмещение аудита ИБ и системы управления качеством

Многие организации, желающие пройти сертификацию на соответствие требованиям BS7799, уже имеют системы управления качеством, сертифицированные по стандартам ISO 9001 или 9002. Аудит системы ИБ можно совместить с сертификацией на соответствие этим стандартам как на первоначальном этапе, так и при контрольных проверках.

Существующие правила требуют, чтобы в таком тестировании принимал участие зарегистрированный аудитор по стандартам BS7799. Планы совместного тестирования должны четко выделять процедуры, связанные с проверкой системы ИБ. Сертифицирующие органы должны гарантировать, что проверке ИБ уделено достаточно времени.

Процедура проведения аудита

Процедура проведения аудита должна начинаться с официального вступительного собрания.

На собрании руководству среднего и верхнего звена и сотрудникам, занимающимся вопросами безопасности, должны быть разъяснены следующие вопросы:

- рамки проведения аудита;
- объяснение методов оценки;
- определение несоответствий и действия по их устранению;
- замечания и возможная реакция на них;
- план проведения аудита;
- доступность документации;
- возможные трудности, которые могут возникнуть в процессе работы — отсутствие ведущих специалистов и т.д.;
- организация работы с конфиденциальными сведениями, необходимыми для проведения аудита, включая отчет о проведении аудита и замечания о несоответствиях. В частности, администрация должна понимать, что аудитору, возможно, потребуется обратиться к потенциально уязвимым участкам системы.

Заключительное собрание с руководителями верхнего звена проводится после проведения аудита. На нем должны быть рассмотрены следующие вопросы:

- подтверждение рамок проведенного аудита;
- краткое изложение найденных несоответствий, согласованных изменений;
- краткое изложение замечаний и предложений;
- общие замечания по ходу аудита и комментарии к отчету;
- выводы: положительное заключение или отказ в сертификации (или продолжение сертификации);
- подтверждение сохранения конфиденциальности сведений, полученных в ходе аудита.

Участники вступительного и заключительного собраний должны быть официально зарегистрированы.

Отчетность

Главным результатом проведения аудита является официальный отчет, в котором должны быть отражены следующие вопросы:

- Соответствие собственным требованиям организации в области ИБ и стандартам BS7799 — согласно плану проведения аудита и Ведомости соответствия.
- Подробная ссылка на основные документы заказчика (по дате или версии), включая:
  - политику безопасности;
  - ведомость соответствия;
  - документы с описанием процедур обеспечения ИБ;
  - дополнительные обязательные или необязательные стандарты и нормы, применяемые к данной организации.
- Общие замечания по выводам проведения аудита.
- Количество и категории полученных несоответствий и замечаний.
- Необходимость дополнительных действий по аудиту (если таковая имеется) и их общий план.
- Список сотрудников, принимавших участие в тестировании.

Этот отчет является официальным документом проведения аудита и его оригинал должен быть доступен сертифицирующему органу. В документе должны быть определены конкретные аспекты обеспечения безопасности (установленные проверяемой организацией и стандартами BS7799), которые будут рассматриваться при каждом посещении. Отчет должен обновляться при каждом проведении аудита.

2.3. Аудит ИБ независимыми организациями, ассоциация ISACA

2.3.1. Ассоциация аудита и управления информационными системами

Ассоциация ISACA основана в 1969 году и в настоящее время объединяет около 20 тыс. членов из более чем 100 стран, в том числе и России. Ассоциация координирует деятельность более чем 12 тыс. аудиторов информационных систем (CICA — Certified Information System Auditor), имеет свою систему стандартов в этой области, ведет исследовательские работы, занимается подготовкой кадров, проводит конференции.

2.3.2. Концепция управления информационными технологиями

Ассоциация развивает свою концепцию управления информационными технологиями в соответствии с требованиями ИБ. На основе этой концепции описываются элементы информационной технологии, даются рекомендации по организации управления, обеспечению режима ИБ. Документ называется CobiT (Control Objectives for Information and Related Technology) и состоит из четырех частей:

- Краткое описание концепции, положенной в основу (Executive Summary).
- Определения и основные понятия (Framework), где определяются основные управляющие процессы для информационной технологии и требования к ним.
- Спецификации управляющих процессов и возможные инструменты воздействия (Control Objectives).
- Рекомендации по выполнению аудита информационной технологии (Audit Guidelines).

Часть, называющаяся Control Objectives, является в некотором смысле аналогом BS7799. Примерно с той же степенью подробности даются практиче-

ские рекомендации по управлению ИБ, однако, модели системы управления ИБ сильно различаются.

Модель управления информационной технологией

CobiT описывает универсальную модель управления информационной технологией (рис. 7). В модели присутствуют ресурсы информационных технологий, являющиеся источником информации, которая используется в бизнес-процессе. Информационная технология должна удовлетворять требованиям бизнес-процесса, которые группируются следующим образом:

- **Требования к качеству технологии** — показатели качества, стоимость, характеристики доставки.

  Показатели качества должны подробно описывать возможные негативные аспекты, которые в обобщенном виде входят в целостность и доступность. Кроме того, включаются и показатели, относящиеся к субъективным аспектам: стиль, удобство интерфейсов и др.

  Характеристики доставки — показатели, в обобщенном виде входящие в доступность и частично конфиденциальность и целостность. Система показателей используется при управлении рисками и оценке эффективности информационной технологии.
- **Доверие к технологии** — соответствие принятым стандартам и требованиям, достоверность информации, действенность.
- **Показатели ИБ** — конфиденциальность, целостность, доступность. Обобщенные показатели для технологии, зависящие от соответствующих показателей качества.

Модель информационной технологии

Любая работающая информационная технология проходит следующие стадии жизненного цикла:

- **Планирование и организация** — определение стратегии и тактики развития информационных технологий, вытекающих из основных целей бизнеса. Затем решаются вопросы, касающиеся реализации: архитектура системы, технологические и организационные аспекты, финансирование и т.д. На данной стадии выделяется 11 основных задач.
- **Приобретение и ввод в действие** — выбранные решения должны быть документально оформлены, спланировано приобретение необходимого оборудования и других средств и ввод их в действие. Выделяется 6 основных задач, решаемых на данной стадии.
- **Доставка и поддержка** — задачи, связанные с обеспечением процесса эксплуатации. Выделяется 13 основных задач, решаемых на данной стадии.
- **Мониторинг** — за процессами, составляющими информационную технологию, необходимо наблюдать и контролировать соответствие их параметров выдвинутым требованиям. Выделяется 4 основные задачи, решаемые на данной стадии.

Итого, выделяется 34 основные задачи (или задачи верхнего уровня), связанные с ресурсами информационных технологий и оказывающие воздействие на отдельные свойства информации, потребляемой бизнес-процессом (рис. 8). Отметим, что кроме традиционных свойств информации: конфиденциальность, целостность, доступность, в данной модели используется еще 4 свойства — действенность, эффективность, соответствие формальным требованиям, достоверность. Эти свойства частично связаны с первыми тремя, (то есть не являются независимыми), их использование можно объяснить соображениями удобства интерпретации результатов.

Далее эта весьма абстрактная схема конкретизируется, каждая из задач подробно расписывается в виде списка существенных аспектов (или точек контроля и управления), которые необходимо проконтролировать. Предлагается 302 точки контроля и управления, позволяющие проверить правильность выполнения этапов.

Для каждой из точек контроля приводятся общие требования и практические рекомендации, каким образом это должно быть выполнено и проконтролировано.

2.3.3. Система стандартов

Действующие стандарты [5-20] приняты в 1998-1999 гг. и размещены на сервере организации: http://www.isaca.org. 12 стандартов объединены в следующие группы:

- Хартия аудитора (Audit Charter) — определяет права и обязанности аудитора.
- Обеспечение независимости (Independence) — гарантии профессиональной независимости аудитора и взаимоотношения с другими организациями.
- Профессиональная этика (Professional ethics and standarts) — требования к профессиональной этике аудиторов и их взаимоотношениям в профессиональной среде.
- Требования к квалификации аудитора (Competence) — формальные требования к знаниям в области технических компонент и другие знания и навыки, необходимые для работы аудитора.
- Требования к повышению квалификации.
- Планирование работ по аудиту(Audit Planning) — документация, предоставляемая аудитору до начала работ и требования, которым должен отвечать план аудита.
- Подотчетность действий аудитора (Performance of audit work) — надзор за действиями аудитора со стороны персонала проверяемой системы (supervision) и корректностью полученных выводов (evidence).

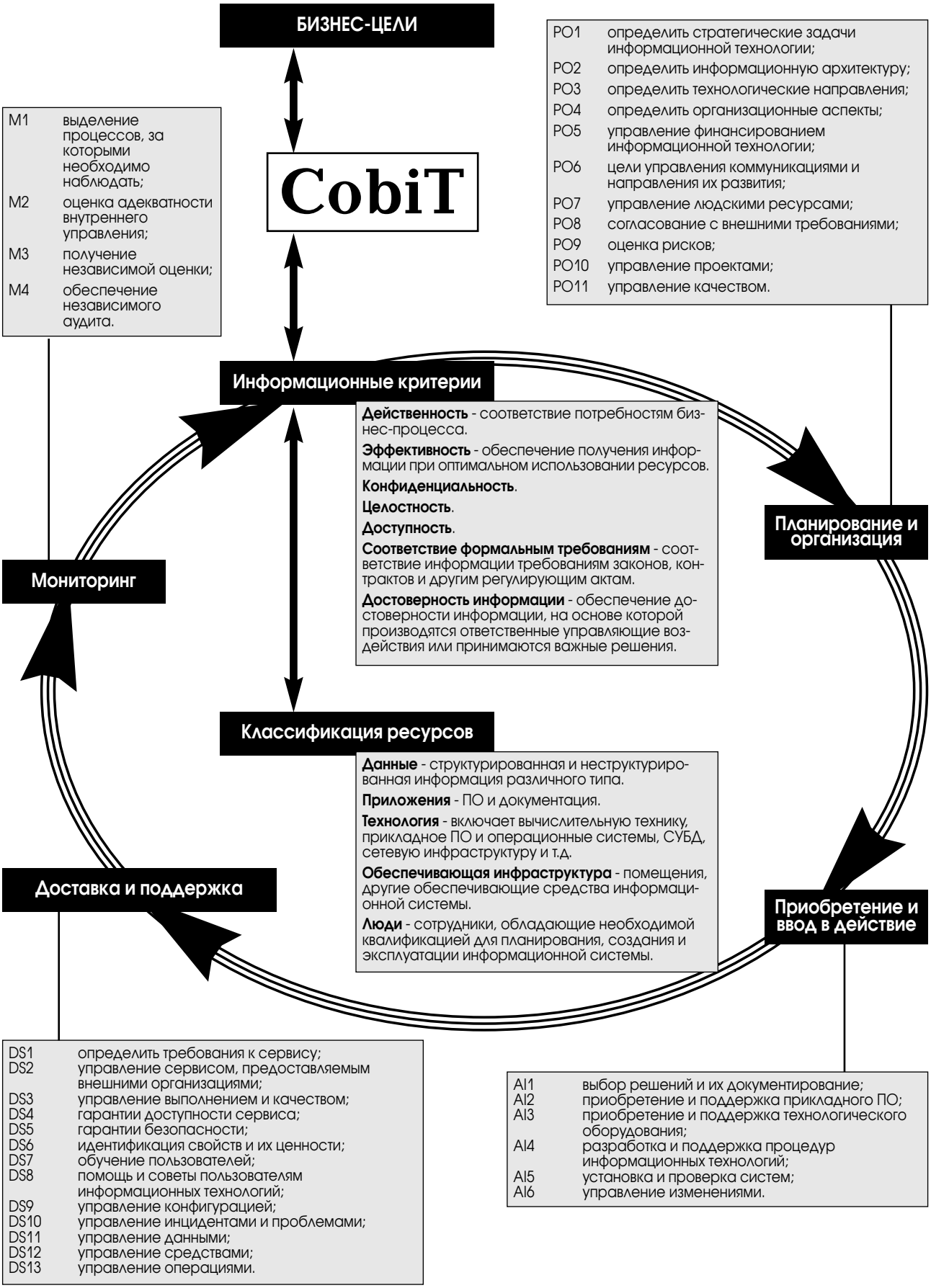

Рис. 7. Модель управления информационной технологией.

П – прямое (сильное) воздействие
О – опосредованное воздействие

Стадии жизненного цикла информационной технологии			Информационные критерии: Действенность	Эффективность	Конфиденциальность	Целостность	Доступность	Соответствие формальным требованиям	Достоверность информации	Классификация ресурсов: Люди	Приложения	Технология	Обеспечивающая инфраструктура	Данные
Планирование и организация Вопросы стратегии и тактики развития информационных технологий, вытекающие из основных целей бизнеса. После того, как цели развития информационных технологий сформулированы, необходимо рассмотреть широкий круг вопросов, касающихся реализации: архитектура системы, технологические и организационные аспекты, финансирование и т.д.	PO1	определить стратегические задачи информационной технологии	П	О						✓	✓	✓	✓	✓
	PO2	определить информационную архитектуру	П	О	О	О					✓			✓
	PO3	определить технологические направления	П	О								✓	✓	
	PO4	определить организационные аспекты	П	О						✓				
	PO5	управление финансированием информационной технологии	П	П					О	✓	✓	✓	✓	
	PO6	цели управления коммуникациями и направления их развития	П					О		✓				
	PO7	управление людскими ресурсами	П	П						✓				
	PO8	согласование с внешними требованиями	П					П	О	✓	✓			✓
	PO9	оценка рисков	О	О	П	П	П	О	О	✓	✓	✓	✓	✓
	PO10	управление проектами	П	П						✓	✓	✓	✓	
	PO11	управление качеством	П	П		П			О	✓	✓			
Приобретение и ввод в действие Для реализации стратегии развития информационной технологии выбранные решения должны быть зафиксированы, спланировано приобретение необходимого оборудования и других средств и ввод их в действие.	AI1	выбор решений и их документирование	П	О							✓	✓	✓	
	AI2	приобретение и поддержка прикладного ПО	П	П		О		О	О		✓			
	AI3	приобретение и поддержка технологического оборудования	П	П		О						✓		
	AI4	разработка и поддержка процедур информационных технологий	П	П		О		О	О	✓	✓	✓	✓	
	AI5	установка и проверка систем	П			О	О			✓	✓	✓	✓	✓
	AI6	управление изменениями	П	П		П	П		О	✓	✓	✓	✓	✓
Доставка и поддержка Включает традиционный набор сервисов, связанных с доставкой	DS1	определить требования к сервису	П	П	О	О	О	О	О	✓	✓	✓	✓	✓
	DS2	управление сервисом, предоставляемым внешними организациями	П	П	О	О	О	О	О	✓	✓	✓	✓	✓
	DS3	управление выполнением и качеством	П	П			О				✓	✓	✓	
	DS4	гарантии доступности сервиса	П	О			П			✓	✓	✓	✓	✓
	DS5	гарантии безопасности			П	П	О	О	О	✓	✓	✓	✓	✓
	DS6	идентификация свойств и их ценности		П					П	✓	✓	✓	✓	✓
	DS7	обучение пользователей	П	О						✓				
	DS8	помощь и советы пользователям информационных технологий	П							✓	✓			
	DS9	управление конфигурацией	П				О		О		✓	✓	✓	
	DS10	управление инцидентами и проблемами	П	П			О			✓	✓	✓	✓	✓
	DS11	управление данными				П			П					✓
	DS12	управление средствами				П	П						✓	
	DS13	управление операциями	П	П		О	О			✓	✓		✓	✓
Мониторинг За всеми процессами, составляющими информационную технологию, необходимо наблюдать и контролировать соответствие их параметров выдвинутым требованиям.Для этого можно использовать как объективные методы, так и экспертные процедуры.	M1	выделение процессов, за которыми необходимо наблюдать	П	О	О	О	О	О	О	✓	✓	✓	✓	✓
	M2	оценка адекватности внутреннего управления	П	П	О	О	О	О	О	✓	✓	✓	✓	✓
	M3	получение независимой оценки	П	П	О	О	О	О	О	✓	✓	✓	✓	✓
	M4	обеспечение независимого аудита	П	П	О	О	О	О	О	✓	✓	✓	✓	✓

Рис. 8. Основные задачи, рассматриваемые в модели CobiT.

- Требования к документации (Reporting) — форма отчета и его содержание.
- Последующие действия (follow-up activites) — надзор за исправлениями, которые вносятся после аудита.

2.3.4. Подготовка кадров и формальные требования к квалификации аудитора

Ассоциация имеет формальные требования к квалификации аудиторов [21], участвует в подготовке кадров необходимой квалификации. Используется двухступенчатая система образования: аудитор должен иметь высшее образование в одной из областей: вычислительной техники, права, учета и пройти курсы повышения квалификации ассоциации. Программа курсов состоит из следующих блоков:

- Базовые знания в области аудита ИБ — теория и практика управления ИБ и аудита, организация бизнес-процессов.
- Спецкурсы — сети, законодательство в области информационных технологий, методы обеспечения безопасности и т.д.
- Информационные технологии в бизнесе — модели и методы исследования бизнес-процессов, обеспечение их ИБ.

После выполнения квалификационной работы выдается диплом аудитора ИБ. Подобные курсы работают при университетах нескольких стран: Австрии, Великобритании, Швеции, США.

2.3.5. Организационные аспекты проведения аудита

Ассоциация уделяет большое внимание регламентации различных аспектов деятельности аудитора. Разумная система регламентации наряду с высокой квалификацией аудиторов обеспечивает качество аудита ИБ. Основным регламентирующим документом является мандат аудитора.

Мандат аудитора

Аудитор CICA имеет мандат на проведение аудита, в котором указаны:

- **Ответственность (Responsibility) и обязанности:**
  - официальное разрешение на проведение работ;
  - цели работ;
  - границы деятельности;
  - объект, на котором проводится аудит;
  - гарантии независимости;
  - специальные требования к проведению аудита;
  - критически важные факторы, обеспечивающие успех мероприятия;
  - отчетные показатели.
- **Полномочия (Authority):**
  - оценивание рисков;
  - право доступа к информации, необходимой для проведения аудита;
  - выбор функций информационной системы (или подсистем), подлежащих аудиту;
  - доступ к необходимым сотрудникам.
- **Подотчетность (Accountability):**
  - отчет должен быть предоставлен руководству организации;
  - основные результаты аудита представляются персоналу;
  - допускается независимая оценка результатов аудита;
  - проверяемые должны быть в курсе действий аудитора;
  - процедура аудита должна соответствовать стандартам и предварительному плану;
  - аудитор отвечает за качество проведения аудита, соблюдение сроков, сметной стоимости и может быть подвергнут штрафу.

2.4. Особенности зарубежных подходов

Современные методы управления ИБ способны обеспечить решение любых корректно поставленных задач в области ИБ, уровень безопасности любой технологии может быть сколь угодно высок.

Наиболее существенные аспекты методик оценки эффективности подсистемы безопасности (в соответствии с BS7799) рассмотрены в приложении. Однако затраты на обеспечение высокого уровня безопасности могут оказаться также чрезвычайно высокими.

Нахождение разумного компромисса, выбор приемлемого уровня безопасности при допустимых затратах является обязательным условием постановки задачи обеспечения ИБ.

Постановка задачи нахождения компромисса между эффективностью подсистемы безопасности и ее стоимостью предполагает, как минимум, что:

- существует система показателей для оценки эффективности подсистемы безопасности и методика их измерения;
- существуют люди (должностные лица), уполномоченные принимать решение о допустимости определенного уровня остаточного риска;
- существует система мониторинга, позволяющая отслеживать текущие параметры подсистемы безопасности.

Наименее формализованный аспект этой задачи — как реально выбрать такой компромисс.

2.4.1. Искусство поиска компромисса

Умение правильно оценить угрозы ИБ в конкретной ситуации, найти систему контрмер, обладающих приемлемым соотношением стоимость/эффективность является одним из необходимых качеств аудитора.

Выбор контрмер с приемлемым значением стоимость/эффективность

В ISACA существуют учебные программы, помогающие овладеть этими навыками. В качестве примера рассмотрим интерактивную обучающую программу TAKO, доступную по адресу http://www.isaca.org/tako.htm.

Пример. Аудит ИБ подсистемы расчета и выдачи зарплаты корпорации

Корпорация, имеющая около 5 тысяч сотрудников, расположена в центральном офисе и 8 филиалах, находящихся в других городах. Расчет зарплаты производится в центральном офисе. Требуется оценить угрозы ИБ, предложить адекватную систему контрмер.

План проведения аудита ИБ предусматривает рассмотрение следующих технологических стадий (рис. 9), решения этой задачи (рис. 9-15 получены с помощью упомянутой выше программы TAKO):

- Учет фактически отработанного сотрудниками времени.
- Передача данных для расчета в центральный офис.
- Работа с массивом персональных данных, используемых при начислении зарплаты.
- Расчет зарплаты.
- Передача платежных ведомостей в банк.
- Отчеты и справки по зарплате.
- Работа с управляющей информацией подсистемы (временные зоны, ставки по категориям, фиксированная часть премиальных и т.д.).

Для каждой стадии составляется список факторов риска, эксперту предлагается выбрать наиболее значимый фактор и ранжировать остальные. Затем рассматриваются возможные контрмеры, характеризуемые стоимостью и эффективностью. Требуется подобрать набор мер с оптимальным (по мнению аудитора) соотношением стоимость/эффективность.

Рассмотрим, например, технологическую стадию: работа с массивом персональных данных, используемых при начислении зарплаты (рис. 10).

Был использован следующий набор угроз:

- T1 — Данные вводит неавторизованный пользователь (оператор).
- T2 — Данные, используемые для выдачи зарплаты, посылаются в банк с неверными банковскими реквизитами.
- T3 — Оператором вводятся фиктивные данные на несуществующих людей (мошенничества с получением денег за несуществующих сотрудников).
- T4 — Несанкционированный доступ (на чтение) к платежным документам внешним нарушителем.
- T5 — В бухгалтерию поступают фальсифицированные платежные ведомости.
- T6 — Информация в базе изменяется в результате телефонного разговора, данные оказываются некорректными.
- T7 — Частично отсутствуют необходимые для начисления зарплаты данные.
- T8 — Описки в количестве нулей — по ошибке оператора размер зарплаты сотрудника увеличивается в 10 раз.
- T9 — Банковские реквизиты в базе данных некорректны.

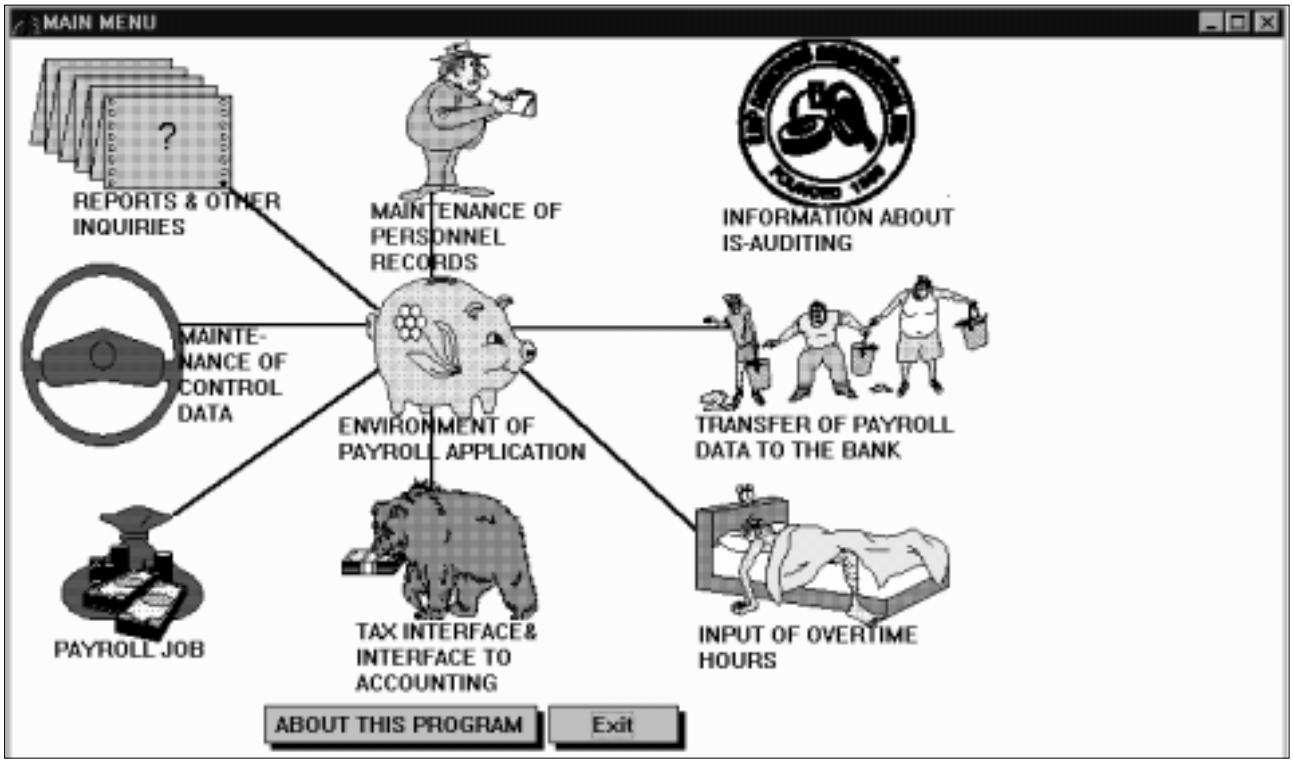

Рис. 9. Стадии проведения аудита ИБ подсистемы расчета и выдачи зарплаты.

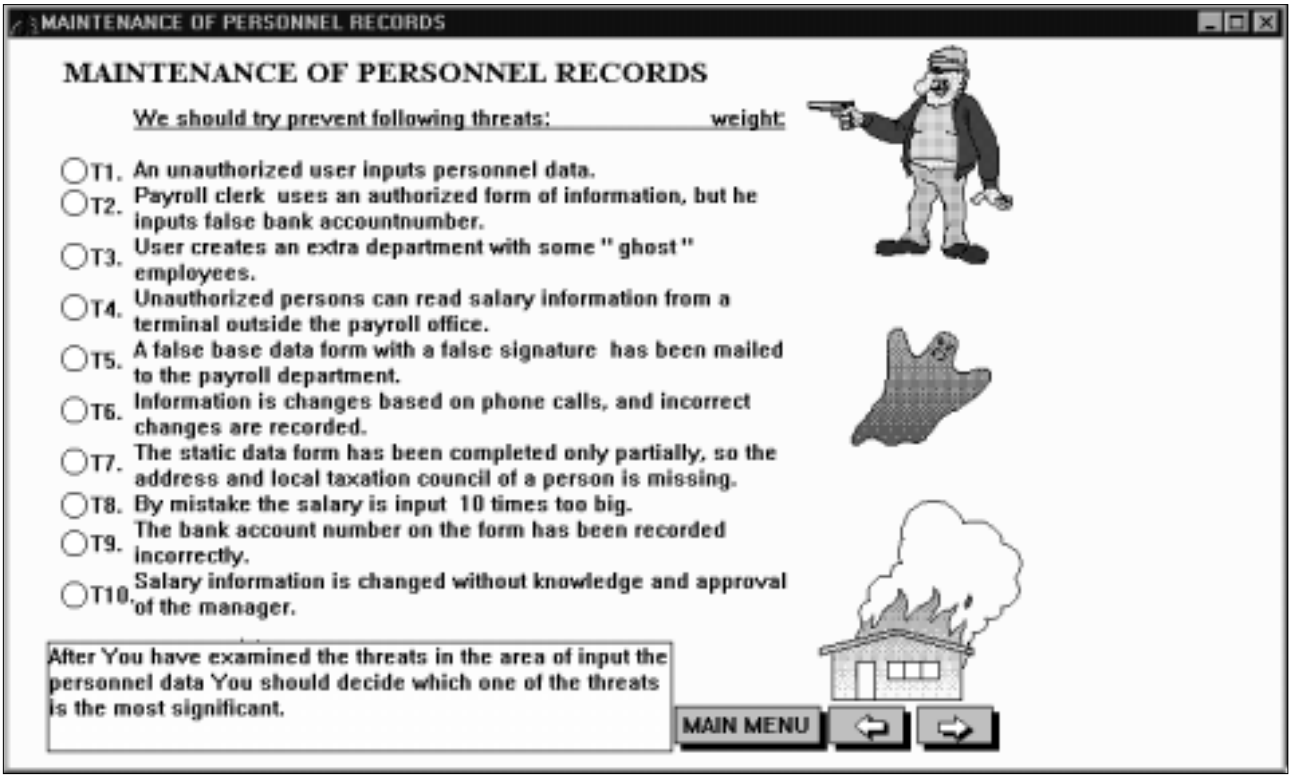

Рис. 10. Угрозы безопасности при работе с массивом персональных данных.

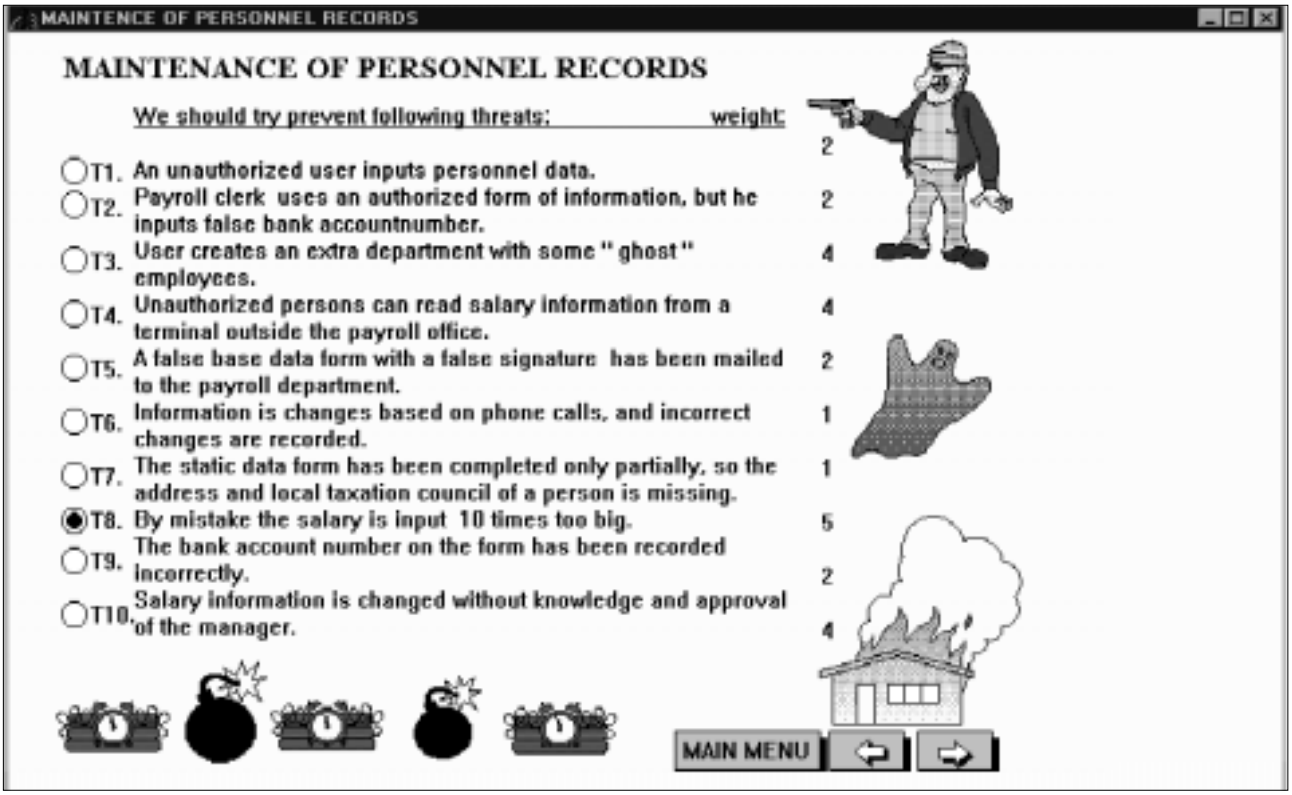

Рис. 11. Ранжирование угроз безопасности.

- T10 — Информация, на основе которой начисляется зарплата, изменяется без уведомления ответственного за это лица.

Аудитору предлагается выбрать наиболее значимую (вероятную) угрозу. Правильным ответом является: ошибки оператора (T8), остальные угрозы могут быть ранжированы так, как показано на рис. 11.

Затем выбирается подходящий набор контрмер из следующего списка (рис. 12):

- Доступ к базе данных по расчету зарплаты предоставляется только имеющему к этому отношение персоналу.
- Другие пользователи должны одобрить вносимые изменения.

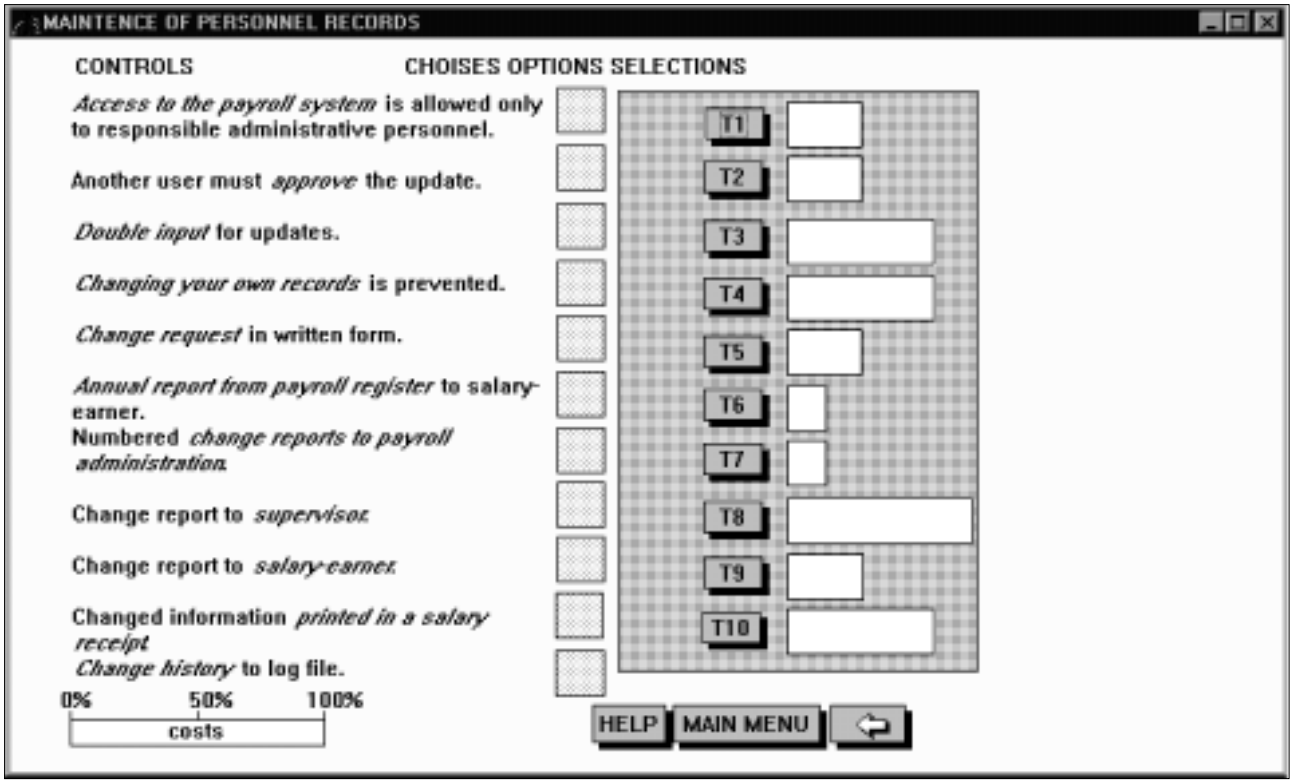

Рис. 12. Набор контрмер.

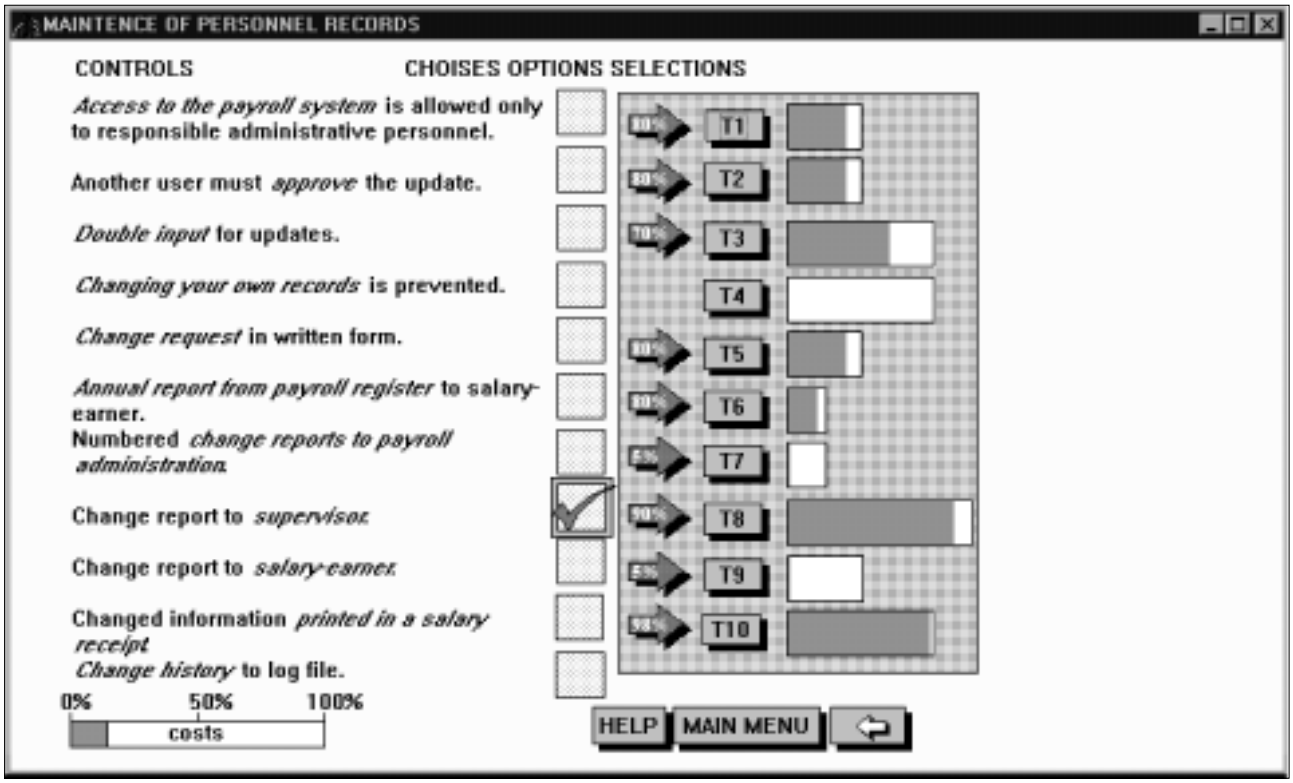

Рис. 13. Эффективность просмотра журнала изменений.

- Двойной ввод при внесении изменений.
- Отсутствует возможность изменения данных на себя любым сотрудником.
- Запрос на изменение данных делается в письменном виде.
- Ежегодный отчет о выданной зарплате по получателям.
- Ведение журнала изменений базы данных бухгалтерии администратором.
- Журнал изменений направляется контролеру.
- Об изменениях базы данных сообщается получателю зарплаты.
- Информация об изменениях вносится в распечатку по расчету зарплаты.

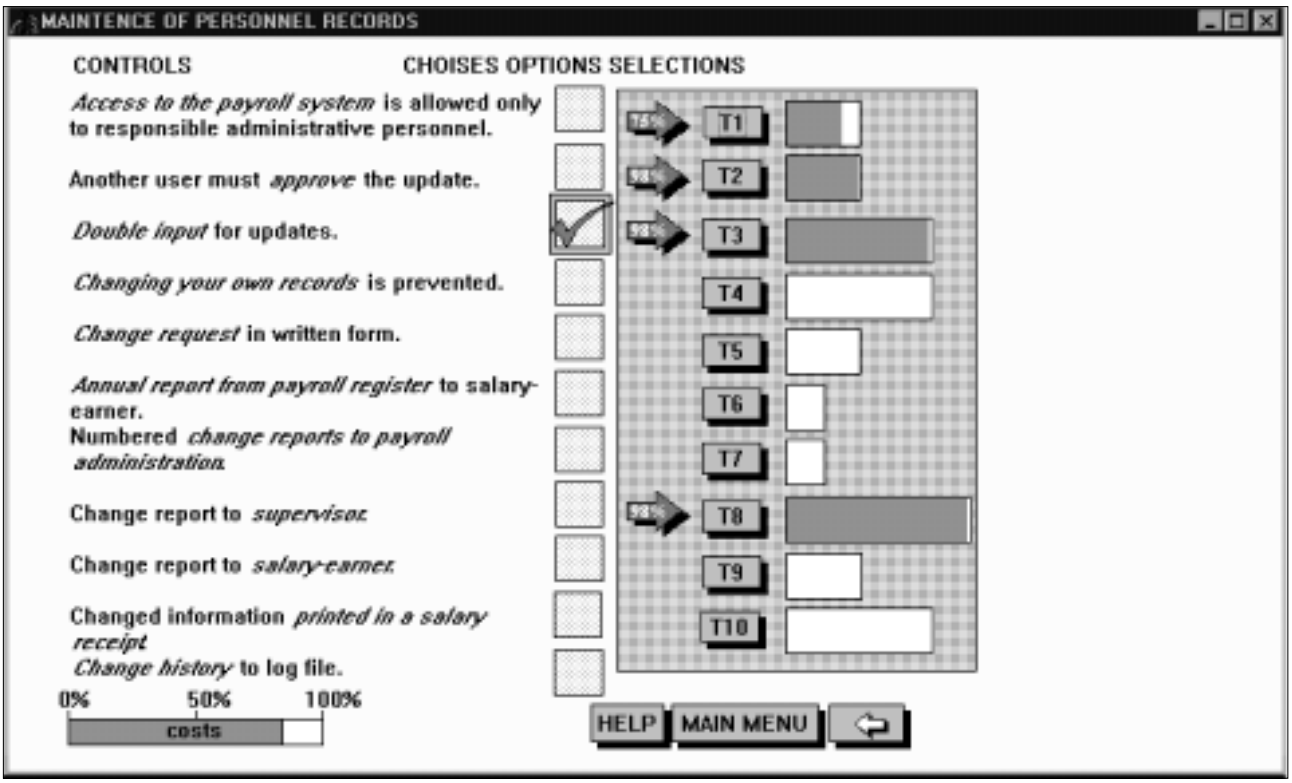

Рис. 14. Эффективность дублирования ввода при внесении изменений.

• Журнал изменений сохраняется в файле.

Каждая из контрмер требует некоторых затрат и уменьшает вероятность реализации нескольких угроз. Аудитор выбирает набор контрмер, обладающий подходящим соотношением стоимость/эффективность.

Например, сравнительно дешевая контрмера — просмотр журнала изменений контролером — является достаточно эффективной. Она уменьшает вероятности реализации практически всех угроз (рис. 13), а более дорогая контрмера — двойной ввод при внесении изменений — в этом смысле менее эффективна рис. 14).

Подходящий по соотношению стоимость/эффективность набор контрмер может выглядеть следующим образом (рис. 15). На рисунке указан дополнительный эффект применения первой контрмеры.

3. Российские нормативные документы

3.1. Российские нормативные документы, регламентирующие вопросы сертификации и аттестации по требованиям ИБ

В 1993-1996 гг. была опубликована серия законов, постановлений правительства и нормативных документов Гостехкомиссии [31-42], в которых рассмотрены вопросы сертификации и аттестации по требованиям ИБ.

3.1.1. Терминология

Вначале рассмотрим основные определения, использованные в этих документах.

- **Сертификация средств защиты информации.** Под сертификацией средств защиты информации по требованиям безопасности информации понимается деятельность по подтверждению их соответствия требованиям государственных стандартов или иных нормативных документов по защите информации, утвержденных Гостехкомиссией России [34].
- **Объекты информатизации.** Под объектами информатизации понимаются автоматизированные системы (АС) различного уровня и назначения, системы связи, отображения и размножения документов вместе с помещениями, в которых они установлены.
- **Аттестация объектов информатизации по требованиям ИБ.** Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России [35].

Система аттестации объектов информатизации по требованиям безопасности является составной частью единой системы сертификации и подлежит государственной регистрации в установленном Госстандартом России порядке.

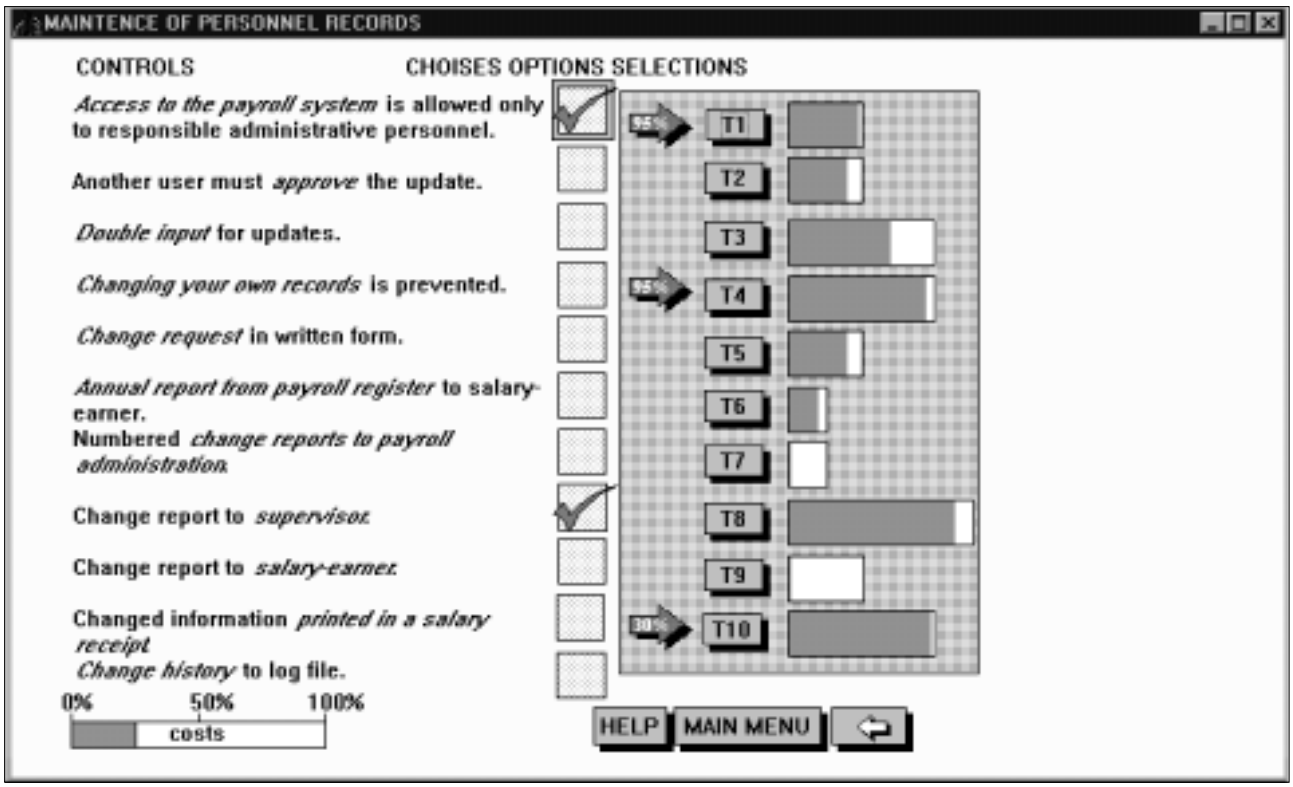

Рис. 15. Суммарная эффективность набора контрмер.

Организационная структура систем сертификации и аттестации приводится на рис. 16, функции определены в РД Гостехкомиссии [34, 35].

3.1.2. Система сертификации

Целями создания системы сертификации являются:

- обеспечение реализации требований государственной системы защиты информации;
- создание условий для качественного и эффективного обеспечения потребителей сертифицированными средствами защиты информации;
- обеспечение национальной безопасности в сфере информатизации;
- содействие формированию рынка защищенных информационных технологий и средств их обеспечения;
- формирование и осуществление единой научно-технической и промышленной политики в сфере информатизации с учетом современных требований по защите информации;
- поддержка проектов и программ информатизации.

Система сертификации средств защиты информации по требованиям ИБ включает в себя и аттестацию объектов информатизации по требованиям ИБ и подлежит государственной регистрации в установленном Госстандартом России порядке.

Обязательной сертификации подлежат средства, в том числе иностранного производства, предназначенные для защиты информации, составляющей государственную тайну, и другой информации с ограниченным доступом, а также средства, использующиеся в управлении экологически опасными объектами. Перечень средств защиты информации, подлежащих обязательной сертификации приведен в [38].

Добровольная сертификация осуществляется по инициативе разработчика, изготовителя или потребителя средства защиты информации.

Порядок проведения сертификации включает:

- подачу и рассмотрение заявки на сертификацию средств защиты информации;
- испытания сертифицируемых средств защиты информации и аттестация их производства;
- экспертизу результатов испытаний, оформление, регистрацию и выдачу сертификата и лицензии на право использования знака соответствия;
- осуществление государственного контроля и надзора, инспекционного контроля за соблюдением правил обязательной сертификации и за сертифицированными средствами защиты информации;
- информирование о результатах сертификации средств защиты информации;
- рассмотрение апелляций.

3.1.3. Аттестация объектов информатизации

Вопросы, связанные с аттестацией объектов информатизации, рассмотрены в [35], [36], [39], [40].

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа — «Аттестата соот-

ветствия» — подтверждается, что объект соответствует требованиям стандартов или иным нормативно-техническим документам по безопасности информации, утвержденным Гостехкомиссией России. Наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с уровнем секретности (конфиденциальности) и на период, установленными в «Аттестате соответствия».

Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

Аттестация проводится органом по аттестации в соответствии со схемой, выбираемой этим органом на этапе подготовки к аттестации из следующего основного перечня работ:

- анализ исходных данных по аттестуемому объекту информатизации;
- предварительное ознакомление с аттестуемым объектом информатизации;
- проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;
- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;
- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;
- проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;
- анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

Имеется типовая методика аттестационных испытаний [39].

Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров.

В остальных случаях аттестация носит добровольный характер (добровольная аттестация) и может осуществляться по инициативе заказчика или владельца объекта информатизации.

Аттестация по требованиям безопасности информации должна предшествовать началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты информации.

Органы по аттестации аккредитуются Гостехкомиссией России. Правила аккредитации определяются в [36], [37].

3.2. Совместимость зарубежных и российских стандартов

Наиболее существенными отличиями зарубежных стандартов являются:

- Формализация этапов выбора и описания целей, которые ставятся в области ИБ для конкретной информационной системы. Используются механизмы оценки соответствия декларированных целей существующим показателям ИБ. В Российских РД предлагается фиксированный набор целей.
- Учет аспектов, связанных с рисками. Это позволяет оптимизировать построение подсистемы безопасности по критериям цена/эффективность.

Организационная структура систем сертификации и аттестации в России

Система сертификации

Гостехкомиссия России
Федеральный орган по сертификации средств защиты информации

Центральный орган системы сертификации средств защиты информации

Органы по сертификации средств защиты информации

Испытательные центры (лаборатории)

Заявители (разработчики, изготовители, поставщики, потребители средств защиты информации)

Система аттестации

Гостехкомиссия России
Федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям ИБ

Органы по аттестации объектов информатизации по требованиям ИБ

Испытательные центры (лаборатории) по сертификации продукции по требованиям ИБ

Заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации)

Рис. 16. Организационная структура систем сертификации и аттестации в России.

- Лучший учет таких аспектов ИБ как целостность и доступность. Российские РД, в основном, ориентированы на обеспечение конфиденциальности.
- Большая степень формализации требований к подсистеме ИБ. В современных стандартах и руководствах формальные требования и рекомендации излагаются в нескольких сотнях подразделов. Соответственно методики построения подсистем ИБ более конкретны, процедуры проведения аудита ИБ достаточно формализованы.

Тем не менее стандарты вполне совместимы, поскольку зарубежные стандарты отличаются от соответствующих Российских РД, в основном, большей детализацией многих аспектов.

4. Заключение

Методы управления ИБ интенсивно развиваются. Основные направления развития связаны с совершенствованием:

- методологии выбора и формализации целей в области безопасности;
- инструментария (методик) для построения подсистемы ИБ в соответствии с выбранными целями;
- технологий аудита, позволяющих объективно оценить положение дел в области ИБ.

Эти составляющие неразрывно связаны и должны соответствовать друг другу. Использование современных методов управления ИБ позволяет поддерживать режим ИБ, соответствующий любым корректно сформулированным целям. Обязательной составной частью таких методов является действенная система аудита ИБ.

До недавнего времени лишь сравнительно небольшая доля организаций добровольно проходила аудит ИБ. Сейчас положение меняется. Приведение подсистем ИБ в соответствие с требованиями современных стандартов и добровольная сертификация на соответствие этим требованиям рассматриваются большинством руководителей как основной путь улучшения положения дел в области безопасности.

В российских условиях рассмотренные стандарты также применимы, поскольку отличаются от соответствующих Российских РД в основном большей детализацией многих аспектов. Применимы и процедуры и методы проверки на соответствие этим требованиям.

Подчеркнем, что Гостехкомиссия России постоянно совершенствует нормативную базу информационной безопасности. Выпускаются новые Руководящие документы, изучается опыт зарубежных стран. Линия на гармонизацию национальных и международных стандартов, в том числе в области аудита безопасности информационных систем, представляется правильной и перспективной.

5. Литература

1. Hill S. The IT security answer. — Logica views, issue 4, London, 1999.

2. Симонов С. Анализ рисков, управление рисками. — JetInfo, 1999, 1.

3. Code of practice for Information security management. — British Standard BS7799: 1995.

4. Information security management. Part 2. Specification for information security management systems. — British Standard BS7799, Part 2, 1998.

5. Standards for Information Systems Auditing. — ISACA Standards, 1998.

6. Standards for Information Systems Control Professionals. — ISACA Standards, 1998.

7. Code of Professional Ethics for Information Systems Control Professionals. — ISACA Guidelines, 1998.

8. IS Auditing Guideline: Corporate Governance of Information Systems. — ISACA Guidelines, 1998.

9. IS Auditing Guideline: Planning the IS Audit. — ISACA Guidelines, 1998.

10. IS Auditing Guideline: Using the Work of Other Auditors and Experts. — ISACA Guidelines, 1998.

11. IS Auditing Guideline: Audit Evidence Requirement. — ISACA Guidelines, 1998.

12. IS Auditing Guideline: Report Content and Form. — ISACA Guidelines, 1998.

13. IS Auditing Guideline: Use of Computer-Assisted Audit Techniques. — ISACA Guidelines, 1998.

14. IS Auditing Guideline: Audit Charter. — ISACA Guidelines, 1998.

15. IS Auditing Guideline: Materiality Concepts for Auditing Information Systems. — ISACA Guidelines, 1998.

16. IS Auditing Guideline: Outsourcing of IS Activities to Other Organisations. — ISACA Guidelines, 1998.

17. IS Auditing Guideline: Audit Documentation. — ISACA Guidelines, 1998.

18. IS Auditing Guideline: Audit Sampling. — ISACA Guidelines, 1998.

19. IS Auditing Guideline: Due Professional Care. — ISACA Guidelines, 1998.

20. IS Auditing Guideline: Effect of Pervasive IS Controls. — ISACA Guidelines, 1998.

21. Model Curricula for Information Systems Auditing at the Undergraduate and Graduate Level. — ISACA, 1998.

22. CobiT: Executive Summary. — ISACA, 2nd Edition, 1998.

23. CobiT: Framework. — ISACA, 2nd Edition, 1998.

24. CobiT: Control Objectives. — ISACA, 2nd Edition, 1998.

25. Guide for developing security plans for information technology systems. — NIST Special Publication 800-18. 1998.

26. Information Technology Security Training Requirements: A role and Performance-Based Model. — NIST Special Publication 800-16, 1998.

27. Guide to BS 7799 risk assessment and risk management. — DISC PD 3002, 1998.

28. Guide to BS 7799 auditing. — DISC PD 3004, 1998.

29. Preparing for BS 7799 certification. — DISC PD 3001, 1998.

30. Guide on the selection of BS7799 controls. — DISC PD 3005, 1999.

31. О сертификации продукции и услуг. — Закон РФ от 10.06.93 N 5151-1.

32. О сертификации средств защиты информации. — Постановление правительства РФ от 26.06.95 N 608.

33. Система сертификации средств криптографической защиты информации (Система сертификации СКЗИ). — Москва, 1993.

34. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. №608 «О сертификации средств защиты информации»). — Гостехкомиссия России, Москва, 1996.

35. Положение по аттестации объектов информатизации по требованиям безопасности информации. — Гостехкомиссия России, Москва, 1994.

36. Положение об аккредитации органов по аттестованию объектов информатики, испытательных центров и органов по сертификации продукции по требованиям безопасности информации. — Гостехкомиссия России, Москва, 1994.

37. Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации. — Гостехкомиссия России, Москва, 1994.

38. Перечень средств защиты информации, подлежащих сертификации в Системе сертификации Гостехкомиссии России. — Гостехкомиссия России, Москва, 1995.

39. Аттестационные испытания АС по требованиям безопасности информации. Типовая методика испытаний объектов информатики по требованиям безопасности информации (Аттестация АС). — Гостехкомиссия России, Москва, 1995.

40. Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации. — Гостехкомиссия России, Москва, 1994.

41. Положение о государственном лицензировании деятельности в области защиты информации. — Гостехкомиссия России, ФАПСИ, Москва, 1997.

42. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. — Москва, 1992.

Приложение 1. Термины и определения

Термины из Руководящих документов Гостехкомиссии России

Под сертификацией средств защиты информации по требованиям безопасности информации понимается деятельность по подтверждению их (средств) соответствия требованиям государственных стандартов или иных нормативных документов по защите информации, утвержденных Гостехкомиссией России.

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России.

Термин Ассоциации аудита и управления информационными системами (ISACA)

Аудит ИБ в информационной системе — процесс сбора сведений, позволяющих установить:

- обеспечивается ли безопасность ресурсов организации (включая данные);
- обеспечиваются ли необходимые параметры целостности и доступности данных;
- достигаются ли цели организации в части эффективности информационных технологий.

Термины Национального института стандартов (NIST) США

Сертификация (Certification) — подтверждение соответствия заявленных и фактических технических характеристик в области ИБ для приложений, компьютерных систем, инфраструктуры.

Аккредитация (Accreditation) — разрешение использования информационной системы общего применения или специализированных приложений (имеющих специальные требования в области ИБ) для обработки информации. Основанием для выдачи разрешения является сертификация уполномоченными специалистами выбранных решений на соответствие заданным требованиям в области ИБ.

Разрешение на использование технологии обработки информации (Authorize Processing) — выдача разрешения упролномоченным лицом, предполагающая осознанное принятие рисков, связанных с использованием данной технологии. Технология обработки информации должна быть построена в соответствии с общими принципами обеспечения ИБ на организационном и программно-техническом уровне.

Ответственный за выдачу разрешения (Designated Approving Authority) — лицо, уполномоченное принять решение о допустимости опреде-

ленного уровня рисков для рассматриваемой информационной системы или технологии обработки информации.

Приложение 2. Аудит ИБ в соответствии с BS7799. Основные положения методики, средства и методы аудита

Рассмотрим основные положения методики проведения аудита [27], [28] и рекомендованные средства и методы оценки рисков. Эти рекомендации вполне применимы и к отечественным условиям и могут быть использованы при разработке соответствующих методик. Особенно полезными представляются приведенные простейшие методы оценки и управления рисками, не требующие использования сложного и дорогостоящего ПО.

Подготовка к сертификации в соответствии с BS7799

Возможны два варианта: сертификация организации в целом и сертификация только информационной системы.

В первом случае организация должна подготовить для проверки:

- Организационную инфраструктуру ИБ на местах — распределение обязанностей сотрудников по обеспечению безопасности.
- Документированную политику информационной безопасности и, в частности, документированный подход к оцениванию и управлению рисками в рамках всей организации.
- Документацию с описанием подходов к оцениванию и управлению рисками.
- Обоснования выбора средств защиты для рассматриваемой системы.
- Процедуру принятия уровня остаточного риска.
- Процедуру проверки режима информационной безопасности и журналов, в которых фиксируются результаты проверки. Это должно подтвердить, что реализованы необходимые средства обеспечения информационной безопасности, тестирование было проведено должным образом, и что они используются корректно.
- Документацию на процессы обслуживания и администрирования информационной системы.
- Документацию по подготовке периодических проверок по оцениванию и управлению рисками.
- Документацию по системе управления информационной безопасностью и реестр средств управления безопасностью в документе «Ведомость соответствия».
- Результаты оценивания рисков по информационной системе.
- Контрмеры для противодействия выявленным рискам.

Эти проверки выполняются с использованием принятых в организации подходов к оценке и управлению рисками.

Во втором случае (сертификация только информационной системы) организация должна подготовить для проверки:

- Документацию по проведенному оцениванию рисков.
- Документацию по средствам управления ИБ, адекватным имеющимся рискам.
- Доказательства эффективности использованных контрмер и результаты их тестирования.
- Политику информационной безопасности, документацию по системе управления информационной безопасностью и документ «Ведомость соответствия».

Подготовка аудитора к проведению сертификации

При проведении подготовительного этапа, необходимого для сертификации всей организации в целом, сотрудник, выполняющий данную работу, должен собрать доказательства того, что организация отвечает всем требованиям, указанным выше. Это делается на основе анализа документов, бесед с экспертами и т.д. Проверяется:

Показатель (ценность) ресурса	Уровень угрозы								
	Низкий			Средний			Высокий		
	Уровни уязвимостей			Уровни уязвимостей			Уровни уязвимостей		
	Н	С	В	Н	С	В	Н	С	В
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Табл. 1. Уровни рисков, соответствующих показателям ресурсов, угроз и уязвимостей.

- наличие соответствующей организационной инфраструктуры безопасности на местах, с установленными обязанностями по обеспечению ИБ для сотрудников всех должностей;
- наличие документированной политики и стратегии информационной безопасности для всей организации в целом, и, в частности, документированной стратегии и общих положений подхода к оцениванию и управлению рисками;
- наличие документированных методик по оцениванию и управлению рисками, или методов, отвечающих установленным критериям, и процедур, гарантирующих их использование на практике;
- обоснование правильности выбора средств защиты для рассматриваемой информационной системы;
- наличие соответствующих процедур принятия уровня остаточного риска документированных процедур проверки режима информационной безопасности и журналов, в которых фиксируются результаты проверки;
- наличие документированных процессов обслуживания и администрирования информационной системы;
- наличие документированных распоряжений должностных лиц по проведению периодических проверок оценивания и управления рисками;
- наличие документации по системе управления информационной безопасностью и реестра необходимых средств обеспечения информационной безопасности в документе «Ведомость соответствия».

Сотрудник, ведущий подготовку к сертификации должен, по меньшей мере, выполнить выборочные проверки выводов, сделанных при оценивании рисков. Для каждого случая нужно:

- подтвердить, что все, что подверглось выборочной проверке, имеет документацию в должном объеме;
- проверить, что оценивание рисков было выполнено в соответствии с корректными методиками;
- подтвердить, что результаты по оцениванию рисков документированы надлежащим образом, достоверны и могут быть использованы;
- подтвердить, что средства обеспечения ИБ, выбранные на основе BS 7799 соответствуют рассматриваемым рискам и документированы соответствующим образом;
- подтвердить, что средства обеспечения ИБ используются правильно и прошли соответствующее тестирование;
- подтвердить, что сотрудники знакомы с политикой ИБ, система управления ИБ надлежащим образом документирована и подготовлен документ «Ведомость соответствия» (в котором описаны риски, используемые законодательные и нормативные требования, указаны выбранные средства обеспечения ИБ и обоснован их выбор);
- стандартным образом оформить свои заключения.

При проведении сертификации только информационной системы сотрудник, ведущий подготовку к сертификации должен:

- Подтвердить, что вопросы, рассматриваемые в ходе проведения периодических проверок системы управления ИБ надлежащим образом документированы.
- Подтвердить, что оценка рисков была произведена корректно или методами, основанными на настоящем руководстве.
- Подтвердить, что результаты оценивания рисков достоверны, приемлемы и документированы должным образом.
- Подтвердить, что необходимые средства обеспечения ИБ были установлены корректно, прошли тестирование и правильно используются.
- Подтвердить, что сотрудники знакомы с политикой ИБ, система управления ИБ должным образом документирована и подготовлен документ «Ведомость соответствия».
- Стандартным образом оформить свои заключения.

Дескриптор угрозы (a) воздействия	Показатель негативного угрозы (c) ресурса) (b)	Реальность реализации	Показатель риска (d)	Ранг угрозы (e)
Угроза A	5	2	10	2
Угроза B	2	4	8	3
Угроза C	3	5	15	1
Угроза D	1	3	3	5
Угроза E	4	1	4	4
Угроза F	2	4	8	3

Табл. 2. Ранжирование угроз.

Данные действия построены на положениях, рассмотренных в части 1 документа [4].

Средства и методы аудита

Для выполнения периодических проверок по оцениванию и управлению рисками существует большой набор методов — от самых простых, использующих подходы на основе анкетирования до самых сложных, использующих технологии структурного анализа.

Методы оценки и управления рисками

Процесс оценивания рисков содержит несколько этапов:

- Идентификация ресурса и оценивание его количественных показателей (определение потенциального негативного воздействия на бизнес).
- Оценивание угроз.
- Оценивание уязвимостей.
- Оценивание существующих и предполагаемых средств обеспечения информационной безопасности.
- Оценивание рисков.

На основе оценивания рисков выбираются средства, обеспечивающие режим ИБ. Ресурсы, значимые для бизнеса и имеющие определенную степень уязвимости, подвергаются риску, если по отношению к ним существует какая-либо угроза. При оценивании рисков учитываются потенциальные негативные воздействия от нежелательных происшествий и показатели значимости рассматриваемых уязвимостей и угроз для них.

Риск характеризует опасность, которой может подвергаться система и использующая ее организация. Риск зависит от:

- показателей ценности ресурсов;
- вероятности реализации угроз для ресурсов;
- степени легкости, с которой уязвимости могут быть использованы при существующих или планируемых средствах обеспечения ИБ, которые уменьшают уязвимость слабых мест, вероятность реализации угроз и негативные воздействия.

Цель процесса оценивания рисков состоит в определении характеристик рисков информационной системе и ее ресурсам. На основе таких данных могут быть выбраны необходимые средства управления ИБ.

При оценивании рисков учитывается: ценность ресурсов, оценка значимости угроз, уязвимостей, эффективность существующих и планируемых средств защиты. Другими словами при оценке рисков необходимо рассматривать несколько аспектов, включая воздействие на бизнес-процесс и вероятность событий.

Показатели ресурсов или потенциальное негативное воздействие на деятельность организации можно определять несколькими способами:

- количественными (например, стоимостные);
- качественными (которые могут быть построены на использовании таких понятий, как, например, умеренный или чрезвычайно опасный);
- их комбинацией.

Для того, чтобы конкретизировать определение вероятности реализации угрозы, рассматривается определенный отрезок времени, в течение которого предполагается защищать ресурс. Вероятность того, что угроза реализуется, определяется следующими факторами:

- привлекательностью ресурса (этот показатель используется при рассмотрении угрозы от умышленного воздействия со стороны человека);
- возможностью использования ресурса для получения дохода (этот показатель используется при рассмотрении угрозы от умышленного воздействия со стороны человека);
- технические возможности угрозы, используемые при умышленном воздействии со стороны человека;
- вероятностью того, что угроза реализуется;
- степенью легкости, с которой уязвимость может быть использована.

В настоящее время известно множество методов, построенных на использовании таблиц. Важно, чтобы организация выбрала для себя подходящий метод, который обеспечивал бы воспроизводимые результаты.

Рассмотрим несколько примеров методов, построенных на использовании таблиц.

Табличные методы, учитывающие только стоимостные характеристики ресурсов

В методах данного типа показатели существующих или предлагаемых физических ресурсов оцениваются с точки зрения стоимости их замены или восстановления работоспособности (то есть количественных показателей). Эти стоимостные величины затем преобразуются на основе той же качественной шкалы, которая используется для информационных ресурсов. Существующие или предполагаемые программные ресурсы оцениваются тем же способом, что и физические, на основе определения затрат на их приобретение или восстановление. При этом используется та же шкала, что и для информационных ресурсов. Если обнаружится, что какое-либо прикладное программное обеспечение имеет особенные требования к конфиденциальности или целостности (например, если исходный текст имеет высокую коммерческую ценность), то оценка этого ресурса производится по

той же схеме, что и для информационных ресурсов, то есть в стоимостном выражении.

Количественные показатели информационных ресурсов оцениваются на основании опросов сотрудников компании (владельцев информации), то есть тех, кто может определить ценность информации, определить ее характеристики и степень критичности, исходя из фактического положения дел. На основе результатов опроса производится оценивание показателей и степени критичности информационных ресурсов для наихудшего варианта развития событий. Рассматривается потенциальное воздействие на бизнес-процесс при возможном несанкционированном ознакомлении с информацией, изменении информации, отказе от выполнения обработки информации, недоступности на различные сроки и разрушения.

Процесс получения количественных показателей дополняется методиками оценивания информационных ресурсов с учетом факторов:

- безопасность персонала;
- разглашение частной информации;
- требования по соблюдению законодательных и нормативных положений;
- ограничения, вытекающие из законодательства;
- коммерческие и экономические интересы;
- финансовые потери и нарушения в производственной деятельности;
- общественные отношения;
- коммерческая политика и коммерческие операции;
- потеря репутации организации.

Разрабатывается система показателей в балльных шкалах (пример — четырехбалльная (от 1 до 4), приведенная ниже). Таким образом, количественные показатели используются там, где это допустимо и оправдано, а качественные показателей — там, где количественные оценки затруднены, например, при угрозе человеческой жизни.

Следующей операцией является заполнение пар опросных листов: по каждому из типов угроз и по группе ресурсов, связанной с данной угрозой. Затем оцениваются уровни угроз (вероятности их реализации) и уровни уязвимостей (легкости, с которой реализованная угроза способна привести к негативному воздействию). Оценивание производится в качественных шкалах.

Например, уровень угроз можно оценить по шкале «высокий-низкий». Уровни уязвимостей оцениваются таким же образом. Информацию собирают на основе опроса сотрудников, занимающихся техническими, кадровыми и сервисными вопросами, выезжая на места и анализируя документацию.

Пример. Будем рассматривать следующие типы угроз:

- умышленные несанкционированные действия людей;
- непредвиденные случайности;
- ошибки со стороны персонала;
- аварии оборудования, программного обеспечения и средств связи.

Уровни рисков, соответствующих показателям (ценности) ресурсов, показателям угроз и уязвимостей, относящихся к каждому типу негативных воздействий, сравниваются при помощи матрицы, аналогичной приведенной в табл. 1.

Количественный показатель риска определяется в шкале от 1 до 8. Значения заносятся в таблицу.

Для каждого ресурса рассматриваются относящиеся к нему уязвимые места и соответствующие им угрозы. Если существует уязвимость и нет связанной с ней угрозы, или существует угроза, несвязанная с какими-либо уязвимыми местами, то в такой ситуации рисков нет. (Но нужно проявлять осторожность, если подобная ситуация изменится). Каждая строка в матрице определяется показателем ресурса, а каждый столбец — степенью опасности угрозы и уязвимости.

Например, ресурс имеет показатель 3, угроза имеет степень «высокая», а уязвимость — «низкая». Показатель риска в данном случае будет 5. Предположим, что ресурс имеет показатель 2, например, для модификации, уровень угрозы — низкий, а уровень уязвимости — высокий. Тогда показатель риска будет 4. Размер матрицы, учитывающей количество степеней опасности угроз, степеней опасности уязвимостей и категорий параметров ресурсов, может быть изменен применительно к конкретной организации.

Реализация данного подхода определяется классификацией рассматриваемых рисков. После того, как оценивание рисков было выполнено первый раз, его результаты целесообразно сохранить, например, в базе данных. В дальнейшем осуществить повторное оценивание будет значительно легче.

Ранжирование угроз

В матрице или таблице можно наглядно отразить связь факторов негативного воздействия (показателей ресурсов) и вероятностей реализации угрозы (с учетом показателей уязвимостей).

На первом шаге оценивается негативное воздействие (показатель ресурса) по заранее определенной шкале, например, от 1 до 5, для каждого ресурса, которому угрожает опасность (колонка b в таблице). На втором шаге по заранее заданной шкале, например, от 1 до 5, оценивается реальность реализации каждой угрозы. На третьем шаге вычисляется показатель риска (при помощи умножения b на c), по которому и производится ранжирование (колонка e). В этом примере (табл. 2) для наименьшего негативного воздействия и для наименьшей реальности реализации выбран показатель 1.

Данная процедура позволяет сравнивать и ранжировать по приоритету угрозы с различными негативными воздействиями и вероятностями реализации. В определенных случаях дополнительно могут потребоваться стоимостные показатели.

Уровень угрозы								
Низкий			Средний			Высокий		
Уровни уязвимостей			Уровни уязвимостей			Уровни уязвимостей		
Н	С	В	Н	С	В	Н	С	В
0	1	2	1	2	3	2	3	4

Табл. 3. Показатель частоты повторяемости.

Оценивание показателей частоты повторяемости и возможного ущерба от риска

Рассмотрим пример оценки негативного воздействия от нежелательных происшествий. Эта задача решается при помощи оценивания двух значений: для каждого ресурса и риска, которые вместе и определяют показатель для каждого ресурса. После того, как баллы всех ресурсов данной системы суммируются, определяется количественный показатель риска для информационной системы.

Вначале каждому ресурсу присваивается определенное значение, соответствующее потенциальному ущербу от воздействия угрозы. Такие показатели присваиваются ресурсу по отношению ко всем возможным угрозам.

Далее оценивается показатель частоты повторяемости. Частота зависит от вероятности возникновения угрозы и степени легкости, с которой может быть использована уязвимость. В результате получается таблица, аналогичная табл. 3.

Затем определяется показатель пары ресурс/угроза. Это делается по таблице, приведенной ниже (см. табл. 4) — показатели ресурса и угрозы суммируются.

На заключительном этапе суммируются все итоговые баллы по всем ресурсам системы и формируется ее общий балл. Его можно использовать для выявления тех элементов системы, защита которых должна быть приоритетной.

Показатель ресурса	Показатель частоты				
	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Табл. 4. Показатели пары ресурс/угроза.

Разделение рисков на приемлемые и неприемлемые

Еще один способ оценивания рисков состоит в разделении их только на допустимые и недопустимые. Возможность применения такого подхода основывается на том, что количественные показатели рисков используются только для того, чтобы их упорядочить и определить, какие действия необходимы в первую очередь. Но этого можно достичь и с меньшими затратами.

Матрица, используемая в данном подходе, содержит не числа, а только символы Д (риск допустим) и Н (риск недопустим). Например, может быть использована матрица из табл. 5.

Вопрос о том, как провести границу между допустимыми и недопустимыми рисками, решается пользователем.

Показатель ресурса	Показатель частоты				
	0	1	2	3	4
0	Д	Д	Д	Д	Н
1	Д	Д	Д	Н	Н
2	Д	Д	Н	Н	Н
3	Д	Н	Н	Н	Н
4	Н	Н	Н	Н	Н

Табл. 5. Разделение рисков на допустимые и недопустимые.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Галатенко В.А. *(galat@jet.msk.su)*
Технический редактор: Антонов А.Н. *(silver@jet.msk.su)*
Россия, 103006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
e-mail: JetInfo@jet.msk.su, http://www.jetinfo.com
Подписной индекс по каталогу Роспечати **32555**