ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО ТО 13569— 2007

Финансовые услуги

РЕКОМЕНДАЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ISO TR 13569:2005
Financial services — Information security guidelines
(IDT)

Издание официальное

БЗ 12—2007/461

Москва
Стандартинформ
2009

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0 — 2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России») и обществом с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (ООО «НПФ «Кристалл») на основе собственного аутентичного перевода стандарта, указанного в пункте 5

2 ВНЕСЕН Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2007 г. № 514-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 Настоящий стандарт идентичен международному стандарту ИСО/МЭК ТО 13569:2005 «Финансовые услуги. Рекомендации по информационной безопасности» (ISO/IEC TR 13569:2005 «Financial services — Information security guidelines»).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении Е

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомления и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2009

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 1
3 Термины и определения . . . 1
4 Обозначения и сокращения . . . 6
5 Политика информационной безопасности организации . . . 6
5.1 Назначение . . . 6
5.2 Правовое и нормативное соответствие . . . 6
5.2.1 Общие положения . . . 6
5.2.2 Требования к финансовым учреждениям . . . 7
5.3 Разработка . . . 10
5.4 Иерархия документации . . . 10
5.4.1 Общий обзор . . . 10
5.4.2 Документы практики обеспечения безопасности . . . 12
5.4.3 Документы операционных процедур обеспечения безопасности . . . 13
6 Менеджмент информационной безопасности. Программа обеспечения безопасности . . . 13
6.1 Общие положения . . . 13
6.2 Создание программы . . . 14
6.3 Осведомленность . . . 14
6.4 Анализ . . . 14
6.5 Менеджмент инцидентов . . . 14
6.6 Мониторинг . . . 14
6.7 Соответствие требованиям . . . 14
6.8 Поддержка . . . 14
6.9 Восстановление после любых прерываний деятельности организации . . . 15
7 Структура информационной безопасности . . . 15
7.1 Приверженность целям организации . . . 15
7.2 Структура организации . . . 15
7.2.1 Роли и обязанности . . . 15
7.2.2 Совет директоров . . . 15
7.2.3 Комитет по аудиту . . . 15
7.2.4 Комитет по менеджменту риска . . . 15
7.2.5 Правовая функция . . . 16
7.2.6 Должностные лица . . . 16
7.2.7 Управляющие делами . . . 16
7.2.8 Сотрудники . . . 16
7.2.9 Сотрудники (персонал), не относящиеся к организации . . . 16
7.2.10 Должности, связанные с безопасностью . . . 17
8 Анализ и оценка риска . . . 18
8.1 Процессы . . . 18
8.2 Процесс оценки риска . . . 19
8.3 Рекомендации по обеспечению безопасности и принятие риска . . . 19
9 Выбор и внедрение защитных мер . . . 19
9.1 Снижение риска . . . 19
9.2 Идентификация и анализ ограничений . . . 20
9.3 Логический контроль доступа . . . 20
9.3.1 Общие положения . . . 20
9.3.2 Идентификация пользователя . . . 20
9.3.3 Санкционирование . . . 21
9.3.4 Аутентификация пользователей . . . 21
9.4 Журнал аудита . . . 22
9.5 Контроль за внесением изменений . . . 22
9.6 Осведомленность об информационной безопасности . . . 22
9.7 Человеческий фактор . . . 23

10 Меры защиты систем информационных технологий . . . 23
10.1 Защита систем информационных технологий . . . 23
10.2 Защитные меры аппаратных систем . . . 23
10.3 Безопасность систем программного обеспечения . . . 24
10.4 Меры защиты сетей и сетевых систем . . . 24
10.5 Меры защиты границ организации и ее связанности с внутренними и внешними сетями . . . 25
10.5.1 Общие положения . . . 25
10.5.2 Межсетевые экраны . . . 25
10.5.3 Система обнаружения вторжений . . . 26
10.5.4 Другие защитные меры противодействия сетевым атакам . . . 26
11 Внедрение специальных средств защиты . . . 27
11.1 Банковские карточки для финансовых операций . . . 27
11.1.1 Общие положения . . . 27
11.1.2 Физическая безопасность . . . 27
11.1.3 Злоупотребление со стороны инсайдеров . . . 27
11.1.4 Перемещение личных идентификационных номеров . . . 27
11.1.5 Персонал . . . 28
11.1.6 Аудит . . . 28
11.1.7 Предупреждение подделки карточек . . . 28
11.1.8 Банкоматы . . . 28
11.1.9 Идентификация и аутентификация владельцев карточек . . . 28
11.1.10 Аутентичность информации . . . 29
11.1.11 Раскрытие информации . . . 29
11.1.12 Предупреждение мошеннического использования банкоматов . . . 29
11.1.13 Техническое обслуживание и текущий ремонт . . . 29
11.2 Системы электронного перевода платежей . . . 29
11.2.1 Несанкционированный источник . . . 29
11.2.2 Несанкционированные изменения . . . 29
11.2.3 Воспроизведение сообщений . . . 30
11.2.4 Сохранение записей . . . 30
11.2.5 Правовая основа платежей . . . 30
11.3 Банковские чеки . . . 30
11.3.1 Общие положения . . . 30
11.3.2 Новые клиенты . . . 30
11.3.3 Вопросы целостности . . . 30
12 Дополнительная информация . . . 30
12.1 Страхование . . . 30
12.2 Аудит . . . 31
12.3 Планирование восстановления деятельности организации после ее прерывания . . . 31
12.4 Внешние поставщики услуг . . . 32
12.5 Группы тестирования на проникновение в компьютерные системы . . . 32
12.6 Криптографические операции . . . 32
12.7 Распределение криптографических ключей . . . 33
12.8 Неприкосновенность частной жизни . . . 33
13 Дополнительные защитные меры . . . 34
13.1 Поддержка функционирования защитных мер . . . 34
13.2 Соответствие требованиям безопасности . . . 35
13.3 Мониторинг . . . 35
14 Разрешение инцидентов . . . 35
14.1 Менеджмент событий . . . 35
14.2 Расследования и правовая экспертиза . . . 36
14.3 Обработка инцидентов . . . 36
14.4 Проблемы, связанные с аварийностью . . . 36

Приложение А (справочное) Образцы документов 37
Приложение В (справочное) Пример анализа безопасности веб-сервисов 42
Приложение С (справочное) Иллюстрация оценки риска 46
Приложение D (справочное) Технологические средства управления 54
Приложение Е (справочное) Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам 59
Библиография 60

Введение

Финансовые услуги как экономическая категория отражают процесс использования денежных средств на основе товарно-денежного обращения. Оказание финансовых услуг за прошедшее десятилетие изменилось как с точки зрения масштабности их осуществления, так и в связи с внедрением компьютерных и сетевых технологий в эту сферу деятельности. При этом подобные операции осуществляются как внутри государства, так и при взаимодействии организаций разных стран.

Настоящий стандарт дает представление о системе обеспечения информационной безопасности в процессе оказания финансовых услуг с учетом сложившейся практики на международном уровне, что особенно важно для организаций, стремящихся развивать свою деятельность за пределами Российской Федерации.

Поправка к ГОСТ Р ИСО/ТО 13569—2007 Финансовые услуги. Рекомендации по информационной безопасности

В каком месте	Напечатано	Должно быть
Обозначение стандарта, на обложке и каждой странице	ГОСТ Р ИСО ТО 13569—2007	ГОСТ Р ИСО/ТО 13569—2007
Обложка	ISO TR 13569:2005	ISO/TR 13569:2005
Предисловие. Пункт 5. Первый абзац	5 Настоящий стандарт идентичен международному стандарту ИСО/МЭК ТО 13569:2005 «Финансовые услуги. Рекомендации по информационной безопасности» (ISO/IEC TR 13569:2005 «Financial services — Information security guidelines»)	5 Настоящий стандарт идентичен международному стандарту ИСО/ТО 13569:2005 «Финансовые услуги. Рекомендации по информационной безопасности» (ISO/TR 13569:2005 «Financial services — Information security guidelines»)

(ИУС № 7 2009 г.)

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Финансовые услуги

РЕКОМЕНДАЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Financial services. Information security guidelines

Дата введения — 2008—07—01

1 Область применения

Настоящий стандарт устанавливает рекомендации по разработке программы обеспечения информационной безопасности для организаций в сфере финансовых услуг. Разработка рекомендаций основывалась на рассмотрении бизнес-среды, практических приемов и процедур деятельности финансовых учреждений. Настоящий стандарт предназначен для использования финансовыми учреждениями различного типа и размера, которые должны разрабатывать рациональную и экономически обоснованную программу обеспечения информационной безопасности.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие международные стандарты:

ИСО 9564 (все части) Банковское дело — Менеджмент и обеспечение безопасности персональных идентификационных номеров

ИСО 10202 (все части) Банковские карточки для финансовых операций — Архитектура безопасности систем финансовых операций, использующих смарт-карты

ИСО 11568 (все части) Банковское дело — Менеджмент ключей (розничная торговля)

ИСО/МЭК 11770 (все части) Информационная технология — Методы и средства обеспечения безопасности — Менеджмент ключей

ИСО 15782 (все части) Менеджмент сертификатов в сфере финансовых услуг

ИСО 16609:2004 Банковское дело — Требования к аутентификации сообщений, используя симметричные методы

ИСО/МЭК 17799:2005 Информационная технология — Практические правила управления информационной безопасностью

ИСО/МЭК 18028 (все части) Информационная технология — Методы и средства обеспечения безопасности — Безопасность информационной сети

ИСО/МЭК 18033 (все части) Информационная технология. — Методы и средства обеспечения безопасности — Алгоритмы шифрования

ИСО 21188:2006 Инфраструктура открытых ключей для сферы финансовых услуг — Практические приемы и структура политики

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **Управление доступом** (access control): Функции, ограничивающие доступ к информации или средствам обработки информации только авторизованным лицам или приложениям, включая физическое

Издание официальное

2—2590

управление доступом, основанное на размещении физических барьеров между неавторизованными лицами и защищаемыми информационными ресурсами, и логические средства управления доступом, использующие другие способы управления.

3.2 **подотчетность** (accountability): Свойство, обеспечивающее однозначное прослеживание действий любого логического объекта.

[ИСО 7498-2:1989] [1], [ИСО/МЭК 13335-1:2004] [2]

3.3 **сигнал тревоги** (alarm): Указание на нарушение безопасности, необычное или опасное состояние, которое может потребовать немедленного внимания.

3.4 **активы** (asset): Все, что имеет ценность для организации [2].

3.5 **аудит** (audit): Служба, задачей которой является проверка наличия адекватных мер контроля и сообщение руководству соответствующего уровня о несоответствиях.

3.6 **журнал аудита** (audit journal): Запись в хронологическом порядке действий системы, содержащей достаточно сведений для того, чтобы реконструировать, проанализировать и проверить последовательность сред и действий, окружающих каждое событие или ведущих к каждому событию по ходу операции от ее начала до выдачи окончательных результатов.

[ИСО 15782-1:2003][3]

3.7 **аутентификация** (authentication): Предоставление гарантии заявленной идентичности объекта.

[ИСО/МЭК 10181-1:1196] [4], [ИСО/МЭК ТО 13335-4:2000] [5]

3.8 **аутентичность** (authenticity): Свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

Примечание — Аутентичность применяется к таким субъектам, как пользователи, к процессам, системам и информации.

3.9 **доступность** (availability): Характеристика, определяющая доступность и используемость по запросу со стороны авторизованного логического объекта [1], [2].

3.10 **резервное копирование** (back-up): Сохранение бизнес-информации для обеспечения непрерывности бизнес-процесса в случае утраты информационных ресурсов.

3.11 **биометрические данные** (biometric): Измеримая биологическая или поведенческая характеристика, с достоверностью отличающая одного человека от другого, используемая для установления либо подтверждения личности человека.

[ANSI X9.84:2003] [6]

3.12 **биометрия** (biometrics): Автоматические методы, используемые для распознавания личности или подтверждения заявленной личности человека на основе физиологических или поведенческих характеристик.

3.13 **метод аутентификации карточек** (МАК) (card authentication method (CAM)): Метод, делающий возможной уникальную машиночитаемую идентификацию банковской карточки для финансовых операций и предотвращающий копирование карт.

3.14 **классификация** (classification): Схема, в соответствии с которой информация подразделяется на категории с целью применения соответствующих защитных мер против этих категорий.

Примечание — Соответствующие защитные меры применяют для следующих категорий: возможность мошенничества, конфиденциальность или критичность информации.

3.15 **конфиденциальность** (confidentialit): Свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса [1], [2], [3].

3.16 **план действий в чрезвычайных обстоятельствах** (contingency plan): Порядок действия, который позволяет организации восстановить работу после природного или иного бедствия.

3.17 **мера управления** (control): По 3.64, термин «защитная мера».

3.18 **политика информационной безопасности организации** [политика] (corporate information security policy) [policy]: Общее положение о намерениях и целях разработки программы обеспечения информационной безопасности организации.

3.19 **кредитный риск** (credit risk): Риск того, что контрагент в системе будет не способен полностью выполнить свои финансовые обязательства в системе в срок или в любое время в будущем.

[CPSS Ключевые принципы для системно значимых платежных систем] [7]

3.20 **критичность** (criticality): Требования к тому, чтобы конкретная информация или средства обработки информации были доступны для ведения бизнеса.

3.21 **криптография** (cryptography): Математический аппарат, используемый для шифрования или аутентификации информации.

3.22 **криптографическая аутентификация** (cryptographic authentication): Аутентификация, основанная на цифровой подписи, коде аутентификации сообщения, генерируемых в соответствии с криптографическим ключом.

3.23 **криптографический ключ** (cryptographic key): Значение, используемое для управления криптографическим процессом, таким как шифрование или аутентификация.

Примечание — Знание соответствующего криптографического ключа дает возможность правильно дешифровать сообщение или подтвердить его целостность.

3.24 **уничтожение информации** (destruction of information): Любое условие, делающее информацию непригодной для использования независимо от причины.

3.25 **цифровая подпись** (digital signature): Криптографическое преобразование, которое, будучи связано с элементом данных, обеспечивает услуги по аутентификации источника, целостности данных и неотказуемости подписавшей стороны.

[ANSI X9.79] [8]

3.26 **раскрытие информации** (disclosure of information): Несанкционированный просмотр или потенциальная возможность несанкционированного просмотра информации.

3.27 **двойной контроль** (dual control): Процесс использования двух или более отдельных логических объектов (обычно людей), действующих совместно для обеспечения защиты важных функций или информации [3].

Примечания

1 Оба логических объекта несут равную ответственность за обеспечение физической защиты материалов, задействованных в уязвимых операциях. Ни один человек в отдельности не может получить доступ к материалам (например, криптографическому ключу) или использовать их.

2 При ручном формировании, передаче, загрузке, хранении и извлечении ключей и сертификатов двойной контроль требует, чтобы каждый из сотрудников знал только часть ключа.

3 При использовании двойного контроля следует позаботиться о том, чтобы обеспечить независимость лиц друг от друга.

3.28 **шифрование** (encryption): Процесс преобразования информации к виду, когда она не имеет смысла ни для кого, кроме обладателей криптографического ключа.

Примечание — Использование шифрования защищает информацию в период между процессом шифрования и процессом дешифрования (который является противоположным шифрованию) от несанкционированного раскрытия.

3.29 **межсетевой экран** (firewall): Совокупность компонентов, помещенных между двумя сетями, которые вместе обладают следующими свойствами:

- весь входящий и исходящий сетевой трафик должен проходить через межсетевой экран;
- пропускается только сетевой трафик, авторизованный в соответствии с локальной политикой безопасности;
- межсетевой экран сам по себе устойчив к проникновению.

3.30 **идентификация** (identification): Процесс установления единственным образом однозначной идентичности объекта [5].

3.31 **образ** (image): Цифровое представление документа для обработки или хранения в системе обработки информации.

3.32 **инцидент** (incident): Любое непредвиденное или нежелательное событие, которое может нарушать деятельность или информационную безопасность [2].

Примечание — К инцидентам информационной безопасности относятся:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политик или рекомендаций;
- нарушение физических защитных мер;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

3.33 **средство(а) обработки информации** (information processing facility): Любая система обработки информации, сервис или инфраструктура, или их физические места размещения [2].

3.34 **информация** (information): Любые данные, представленные в электронной форме, написанные на бумаге, высказанные на совещании или находящиеся на любом другом носителе, используемые финансовым учреждением для принятия решений, перемещения денежных средств, установления ставок, предоставления ссуд, обработки операций и т. п., включая компоненты программного обеспечения системы обработки.

3.35 **информационные активы** (information asset): Информационные ресурсы или средства обработки информации организации.

3.36 **информационная безопасность** (information security): Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки [2].

3.37 **лицо, ответственное за информационную безопасность** (information security officer): Лицо, отвечающее за внедрение и поддержку программы обеспечения информационной безопасности.

3.38 **информационные ресурсы** (information resource): Оборудование, используемое для обработки, передачи или хранения информации, независимо от того, находится оно внутри организации или за ее пределами.

Примечание — К подобному оборудованию относятся: телефоны, факсимильные аппараты и компьютеры.

3.39 **целостность** (integrity): Свойство сохранения правильности и полноты активов [2].

3.40 **ключ** (key): По 3.23, термин «Криптографический ключ».

3.41 **использование фальшивого чека** (kiting): Использование фальшивого чека для получения кредита или денег.

3.42 **правовой риск** (legal risk): Риск потерь из-за непредвиденного применения закона или нормативного акта или из-за невозможности выполнения контракта [7].

3.43 **гарантийное письмо** (letter of assurance): Документ, описывающий меры обеспечения информационной безопасности, применяемые для защиты информации, хранимой по поручению получателя письма.

3.44 **риск ликвидности** (liquidity risk): Риск того, что у контрагента в системе будет недостаточно средств для выполнения своих финансовых обязательств в системе в полном объеме в срок, хотя существует возможность, что он сможет сделать это в какой-то момент в будущем [7].

3.45 **код аутентификации сообщений (КАС)** (message authentication code MAC): Код, который присоединяется к сообщению его автором, являющийся результатом обработки сообщения посредством криптографического процесса.

Примечание — Если получатель может создать такой же код, возникает уверенность в том, что сообщение не было модифицировано и что оно исходит от владельца соответствующего криптографического ключа.

3.46 **модификация информации** (modification of information): Обнаруженное или необнаруженное несанкционированное или случайное изменение информации.

3.47 **принцип необходимого знания** (need to know): Концепция безопасности, ограничивающая доступ к информации и ресурсам обработки информации в объеме, необходимом для выполнения обязанностей данного лица.

3.48 **сеть** (network): Совокупность систем связи и систем обработки информации, которая может использоваться несколькими пользователями.

3.49 **неотказуемость** (non-repudiation): Способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты [1], [2].

[ИСО/МЭК 13888-1:2004] [9]

3.50 **операционный риск** (operational risk): Риск того, что операционные факторы, такие как технические нарушения функционирования или операционные ошибки, вызовут или усугубят кредитный риск или риск ликвидности [7].

3.51 **обладатель информации** (owner of information): Работник или служба, отвечающие за сбор и сохранение данной совокупности информации.

3.52 **пароль** (password): Строка символов, служащая в качестве аутентификатора пользователя.

3.53 **целесообразная бизнес-практика** (prudent business practice): Совокупность практических приемов, которые были в целом признаны как необходимые.

3.54 **достоверность** (reliability): Свойство соответствия предусмотренному поведению и результатам [2]:

3.55 **остаточный риск** (residual risk): Риск, остающийся после его обработки [2].

3.56 **риск** (risk): Потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей актива или группы активов [2].

Примечание — Определяется как сочетание вероятности события и его последствий.

3.57 **принятие риска** (risk acceptance): Решение организации взять риск на себя, связанное с исключением в политике.

3.58 **анализ риска** (risk analysis): Систематический процесс определения величины рисков [2].

3.59 **оценка риска** (risk assessment): Процесс, объединяющий идентификацию риска, анализ риска и оценивание риска [2].

3.60 **оценивание риска** (risk evaluation): Процесс сравнения проанализированных уровней риска с заранее установленными критериями и идентификации областей, где требуется обработка риска.

3.61 **идентификация риска** (risk identification): Процесс идентификации рисков, рассматривающий бизнес-цели, угрозы и уязвимости как основу для дальнейшего анализа.

3.62 **менеджмент риска** (risk management): Полный процесс идентификации, контроля, устранения или уменьшение последствий вероятных событий, которые могут оказать влияние на ресурсы информационно-телекоммуникационных технологий [2].

3.63 **обработка риска** (risk treatment): Процесс выбора и реализации мер по изменению рисков.

3.64 **защитная мера** (safeguard): Сложившаяся практика, процедура или механизм обработки риска [2].

Примечание — Следует заметить, что понятие «защитная мера» может считаться синонимом понятия «мера управления».

3.65 **безопасность** (security): Качество или состояние защищенности от несанкционированного доступа или неконтролируемых потерь или воздействий.

Примечания

1 Абсолютная безопасность является практически недостижимой, а качество определенной системы безопасности — относительным.

2 В рамках системы безопасности «состояние — модель» безопасность является таким «состоянием», которое должно сохраняться при различных операциях.

3.66 **сервер** (server): Компьютер, действующий как поставщик некоторых услуг, таких как обработка коммуникаций, обеспечение интерфейса с системой хранения файлов или печатное устройство.

3.67 **регистрация** (sign-on): Завершение идентификации и аутентификации пользователя.

3.68 **разделенное знание** (split knowledge): Разделение критичной информации на множество частей так, чтобы требовалось наличие минимального числа частей, перед выполнением какого-либо действия.

Примечание — Разделенное знание часто используется для осуществления двойного контроля.

3.69 **карточка хранения ценностей** (stored value card): Устройство, позволяющее хранить и осуществлять операции с электронными деньгами.

3.70 **системный риск** (systemic risk): Риск того, что неспособность одного из участников выполнить свои обязательства либо нарушения в функционировании самой системы могут привести к неспособности других участников системы или других финансовых учреждений в других частях финансовой системы выполнять свои обязательства в срок [7].

Примечание — Подобный сбой может вызвать распространение проблем с ликвидностью или кредитами и в результате поставить под угрозу стабильность системы или финансовых рынков.

3.71 **угроза** (threat): Потенциальная причина инцидента, который может нанести ущерб системе или организации [2].

3.72 **средство идентификации** (token): Контролируемое пользователем устройство (например диск, смарт-карта, компьютерный файл), содержащее информацию, которая может использоваться в электронной торговле для аутентификации или управления доступом.

3.73 **идентификатор пользователя** (user ID): Строка символов, используемая для однозначной идентификации каждого пользователя системы.

3.74 **уязвимость** (vulnerability): Слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами [2].

4 Обозначения и сокращения

КПРС — комитет по платежным и расчетным системам;
FTR — протокол передачи файлов;
http — протокол передачи гипертекста;
HTTPS — протокол защищенной передачи гипертекста;
IP — протокол Интернет;
IPSEC — протокол IPSec;
ИТ — информационная технология;
ПК — персональный компьютер;
PEAP — защищенный расширяемый протокол аутентификации;
PIN — персональный идентификационный номер;
SMTP — простой протокол электронной почты;
SSH — вид терминального доступа к серверу с большей степенью защищенности сеанса связи;
SSL — протокол безопасных соединений;
WS — веб-серверы;
XML — расширяемый язык разметки;
ЕС — Европейский Союз.

5 Политика информационной безопасности организации

5.1 Назначение

Все учреждения финансовых услуг в значительной степени зависят от использования ИТ информационно-коммуникационных технологий и, следовательно, нуждаются в обеспечении защиты информации и менеджменте безопасности своих информационных активов. Следовательно обеспечение информационной безопасности и менеджмент информационной безопасности должны стать важным компонентом плана руководства организации.

Разработка программы обеспечения информационной безопасности является целесообразной бизнес-практикой, помогающей учреждениям, предоставляющим финансовые услуги, идентифицировать и осуществлять менеджмент риска. Настоящий стандарт устанавливает общий, основанный на политике безопасности подход к менеджменту информационной безопасности и рекомендации, которые могут быть адаптированы для бизнес-целей данной организации. Бизнес-целям должны способствовать политики и процедуры обеспечения защиты активов ИТ. Основанный на политике безопасности подход применим к учреждениям с различных масштабов, типов управления и организационных структур.

В настоящем стандарте приводятся общие рекомендации руководству учреждения, предоставляющего финансовые услуги по различным аспектам менеджмента информационной безопасности в разработке и поддержке программы обеспечения информационной безопасности. Другие источники, в частности ИСО/МЭК 17799, предоставляют важную подробную информацию общего назначения, которая окажет неоценимую помощь в вопросах внедрения и поддержки программы обеспечения информационной безопасности. Настоящий стандарт устанавливает конкретные правовые и нормативные требования, которые должны учитываться финансовыми учреждениями при создании, основанной на политике безопасности менеджмента информационной безопасности.

5.2 Правовое и нормативное соответствие

5.2.1 Общие положения

Распорядительные органы в основном занимаются вопросами безопасности, устойчивости и соблюдения законов и положений. Одним из элементов безопасности и устойчивости является система защитных мер организации, которая обеспечивает защиту информации от недоступности, несанкционированного изменения, раскрытия и уничтожения. Последние национальные и международные законы, такие как Базель II [10], закон Сэрбэйнс-Оксли (SOX) [11], закон Грэма-Лича-Блили (GLB) [12] и Европейская директива

95/46/ЕС [13], определили среду правового и регулятивного риска для мировых поставщиков финансовых услуг. Политика безопасности организации должна учитывать этот риск.

Сотрудники, ответственные за обеспечение соответствия требованиям политики безопасности, должны работать вместе с руководителем службы обеспечения информационной безопасности организации, руководителем финансовой службы организации, управляющими делами, лицами, занимающимися менеджментом риска, и аудиторами над тем, чтобы требования информационной безопасности национальных и международных законов и положений были доведены до работников организации и разъяснены им. Ответственные сотрудники за оценку соответствия информационной безопасности должны следить за появлением новых информационных технологий или методологий оценки информационной безопасности, которые могут стать объектом регулирования, например, за соответствием новых продуктов информационных технологий заранее определенным классам функциональных возможностей по информационной безопасности.

5.2.2 Требования к финансовым учреждениям

5.2.2.1 Обзор

Для учреждений финансового сектора существуют определенные правовые требования и нормы, оказывающие влияние на безопасность ИТ, которые должны соблюдаться. Основная проблема заключается в том, что эти требования в разных странах различны. Хотя ЕС проложил путь к устранению различий в правовых нормах, все еще остаются национальные правовые нормы, требующие особого отношения.

Далее описываются наиболее важные законы с точки зрения поставщика финансовых услуг, действующего в глобальных условиях. Описание нормативных требований представлено в виде разделов: «Организационное управление», «Защита данных (неприкосновенность частной жизни)» и «Законодательство финансового сектора», характерное для поставщиков финансовых услуг (например законы, касающиеся легализаций криминальных доходов). Описание законодательной среды основано на требованиях финансовой отчетности и рекомендациях, установленных в [10].

5.2.2.2 Правовые требования

5.2.2.2.1 Руководство организации

В последние годы многие национальные и региональные законодательные органы выдвинули законы, касающиеся руководства организации. Среди них известны следующие: закон Сэрбэйнс-Оксли (SOX) в США, закон Kontrolle- und Transparenz Gesetz (KonTraG) в Германии и проект директивы ЕС «О руководстве организации». Эти три закона изменили систему правовых рисков, с которыми сталкиваются поставщики финансовых услуг.

Закон SOX требует, чтобы все компании, ведущие свободную торговлю на фондовых биржах США, предоставляли свидетельство наличия у них адекватных средств контроля для финансовой отчетности. Говоря более подробно, закон SOX обязывает руководителя компании и руководителя ее финансовой службы проводить оценку эффективности внутренней системы контроля организации, а также принимать на себя всю ответственность за ежегодные финансовые отчеты организации. В этих целях в отношении ИТ необходимо проводить оценку и контроль функционирования критических бизнес-приложений и связанных с ними рисков. Весь жизненный цикл бизнес-приложений — от первоначальной разработки до обеспечения непрерывности бизнеса — должен подвергаться оценке и контролю с целью гарантирования наличия адекватных защитных мер. Хотя этот закон является национальным, его применяют к любой компании, чьи акции свободно продаются в США.

Немецкий закон KonTraG требует от организации внедрения внутреннего процесса мониторинга, определяющего внутренние разработки и решения, которые могут представлять высокий уровень риска для этой организации. Это требование подразумевает, что руководство должно внедрять внутреннюю систему менеджмента риска в масштабе организации. Данный закон также обязывает руководство сообщать об идентифицированном серьезном риске в своей системе отчетности (представляемой дважды в год и ежегодно). В отношении ИТ в нем рассматривается тот же аспект, что в законе SOX. Однако, поскольку немецкие компании, ведущие свободную торговлю, имеют двухуровневый совет директоров, требуется более строгая система отчетности совета директоров наблюдательному совету. Несоответствие данному закону может приводить к снижению банковского рейтинга организации и, следовательно, оказывать влияние на процентные ставки за кредиты.

ЕС разрабатывает проект директивы, который окажет влияние на национальное законодательство ЕС, и заключается в том, что от всех компаний, чьи акции зарегистрированы на фондовой бирже, требуется публикация отчета об управлении организации. Данный отчет должен содержать подробную информацию о совете директоров, его решениях, финансовом положении компании и соблюдении законодательства ЕС. Кроме этого, отчет должен также включать в себя результаты независимых аудитов. Директива имеет похо-

жие следствия для ИТ, что и законы SOX и KonTraG. Существуют и другие национальные законы, но ни один из них не является настолько строгим, чтобы оказывать влияние на директиву ЕС.

5.2.2.2.2 Защита данных (неприкосновенность частной жизни)

Вопрос защиты данных привлекает все больше и больше внимания, что обусловлено различными законами регионального, федерального и государственного уровней. Появление этих законов определено тем, что использование Интернета создает дополнительные риски, касающиеся злоупотребления в этой сфере, и люди, использующие этот носитель информации, нуждаются в соответствующей защите.

Для защиты информации потребителей, хранимой в финансовых учреждениях, предназначен закон GLB [12]. Он требует, чтобы эти учреждения предоставляли своим клиентам уведомление о гарантии неприкосновенности частной жизни, объясняющее практические приемы (практику) учреждений в отношении коллективного использования информации. В свою очередь потребители имеют право на коллективное использование своей информации. Закон также требует, чтобы финансовые учреждения защищали информацию, собранную об отдельных лицах; но не относится к информации, собранной в ходе коммерческой или бизнес-деятельности. Федеральная торговая комиссия (ФТК) опубликовала комплекс стандартов, который должен применяться для обеспечения соответствия закону GLB.

Совместное усилие по достижению неприкосновенности частной жизни для всех стран-участниц на высоком уровне представляет собой [13]. Данная директива защищает информацию о физических лицах во время всего жизненного цикла, проще говоря требует, чтобы любое учреждение запрашивало разрешение в случае использования информации образом, отличным от официального (и утвержденного). Директива также ограничивает передачу персональных данных тем странам, где обеспечивается их неадекватная защита. Физические лица должны давать недвусмысленное разрешение на последующую обработку своей персональной информации. Требования, установленные в директиве, отличаются от процедур в США, где физических лиц не запрашивают о разрешении о запрещении дальнейшей обработки персональной информации. Европейская директива внедряется в национальное законодательство всех стран — членов ЕС.

Швейцарский закон о защите данных [14] идентичен законам других европейских стран. Данный закон упоминается здесь по двум причинам: Швейцария не является частью ЕС. С другой стороны, швейцарский закон запрещает передачу персональных данных в другие страны при отсутствии адекватной защиты и требует от передающей организации информировать о ее передаче орган, отвечающий за защиту персональных данных. Другим важным законом, связанным с финансовыми учреждениями, является закон о тайне вкладов клиентов швейцарского банка (Schweizer Bankkundengeheimnis) [15], обеспечивающий безусловную защиту информации о клиентах, хранимой банками.

5.2.2.2.3 Легализация криминальных доходов

Почти во всех странах имеются законы по борьбе с легализацией криминальных доходов, которые обычно предписывают, чтобы все переводы денег, превышающие определенную сумму, подвергались расследованию с целью проверки их источников и адресата. Еще в 90-х годах такие законы не имели явного отношения к безопасности, так как они применялись на практике без учета решения проблем безопасности.

Атаки террористов, совершенные в США 11 сентября 2001 г., ясно показали важность законов, направленных против легализации криминальных доходов и связанных с ними мер защиты. Эти атаки стимулировали осознание важности сотрудничества в сфере борьбы с легализацией криминальных доходов по всему миру. Это осознание оживило международное сотрудничество и привело к значительным изменениям законов, направленных против легализации криминальных доходов и вносящих свой вклад в способность мирового сообщества отслеживать денежные средства тех, кто финансирует международный терроризм.

С 2001 года США продолжают проводить активную межведомственную международную обучающую программу по борьбе с легализацией криминальных доходов с целью повышения международных усилий по борьбе с легализацией криминальных доходов и финансовыми преступлениями. Правительства США и других стран, а также международные организации тоже усилили свои программы, направленные против легализации криминальных доходов. Европейский Союз расширил свою директиву по борьбе с легализацией криминальных доходов и возложил обязанности противодействия легализации криминальных доходов на «сторожей», профессионалов, таких, как юристы и бухгалтеры, которые должны препятствовать вовлечению криминальных доходов в финансовые системы государств. Продолжают эффективно работать региональные организации по борьбе с легализацией криминальных доходов в Европе, Азии и странах Карибского бассейна и начинают действовать зарождающиеся региональные организации по борьбе с легализацией криминальных доходов в странах Южной Америки и Африки.

Основное внимание в сфере борьбы с легализацией криминальных доходов в 2005 г. сосредоточилось на работе Финансовой оперативной группы (FATF), всемирно признанной международной организации по борьбе с легализацией криминальных доходов, которая продолжила свою работу со странами и территориями, которые не входят в состав международной организации. После 11 сентября 2001 г. FATF быстро отреагировала и созвала чрезвычайное пленарное заседание по вопросу борьбы с финансированием терроризма, принявшее решение расширить свою задачу за рамки борьбы с легализацией криминальных доходов и сосредоточить свою энергию и опыт на мировых усилиях по борьбе с финансированием терроризма. С этого времени FATF приняла восемь специальных рекомендаций по вопросу противодействия финансирования терроризма.

Атаки террористов послужили сильным импульсом для многих стран к внесению изменений и усилению законов по борьбе с легализацией криминальных доходов. В США закон об объединении и укреплении США обеспечением соответствующих средств, необходимых для противодействия терроризму от 2001 года внес значительные изменения в систему борьбы с легализацией криминальных доходов. Новые широкие полномочия, предоставленные этим законом, окажут существенное влияние на взаимоотношения между финансовыми учреждениями США и их индивидуальными клиентами и клиентами на уровне учреждений.

Программа менеджмента информационной безопасности может помочь финансовым учреждениям разрушить схемы легализаций криминальных доходов. И, что более важно, эти программы могут использоваться для демонстрации регулирующим органам и организациям того, что конкретное финансовое учреждение соблюдает законодательство и предоставляет документацию о принятии систематических и активных мер для соблюдения законодательства.

5.2.2.2.4 Законы, относящиеся к финансовым рынкам

Большинство законов, регулирующих финансовый сектор, в основном определяет обязанности финансового учреждения, что включает в себя обязательство по предоставлению квалифицированных услуг. Некоторые органы власти государства интерпретируют это обязательство так, что оно распространяется на всю полноту используемых услуг ИТ. На конкретные вопросы безопасности ИТ указывают следующие законы различных государств.

По аргентинскому банковскому законодательству, финансовые учреждения должны иметь в своем составе руководителя службы обеспечения информационной безопасности (ИСО), который предоставляет ежегодный отчет центральному банку Аргентины. В отчете содержатся требования к осуществлению и поддерживанию внутренних мер защиты финансового учреждения для обеспечения надлежащих услуг.

Директива ЕС 82/121/ЕЭС [16] регулирует отчетность финансовых учреждений и была недавно обновлена для осуществления более регулярной отчетности на всей территории ЕС. Директива ЕС 2000/31/ЕС (об электронной торговле) [17] определяет правовую структуру электронной торговли. Данная директива должна включать в себя вопросы неприкосновенности частной жизни клиентов, регулирование проблем спама, налогообложение, электронные контракты и их обработку, конфиденциальность обмена информацией. Директива также определяет кодекс поведения вовлеченных организаций как средство обмена информацией о правах.

Закон Kreditwesengesetz (KWG) [18] регулирует практически все вопросы, характерные для финансовых учреждений в Германии. Данный закон определяет, как должны функционировать банки, кому разрешается возглавлять финансовое учреждение, что должно содержаться в отчетности и т.д. Три параграфа этого закона представляют особый интерес. В первом рассматривается проблема автоматического доступа финансовых органов к данным клиентов (§ 24c), для которых требуются дополнительные меры безопасности. Во втором (§ 25a) определяются особые обязательства для финансовых учреждений, охватывающие такие вопросы, как менеджмент внутреннего риска, меры безопасности и внутренний аудит, а также их сотрудничество с надзорными органами. Наконец, существуют предписания на случай невыполнения конкретным финансовым учреждением или его руководством своих обязанностей, что может привести к утрате руководством права ведения бизнеса в финансовом секторе.

5.2.2.3 Нормативные требования

Два направления нормативных требований к финансовым учреждениям являются актуальными. Первое направление касается обязательств учреждения по финансовой отчетности (обычно надзор осуществляется национальными финансовыми органами). Вторым направлением является обязательство финансовой устойчивости, которое описывается в [10]. Эти требования включают в себя необходимость рассмотрения финансовым учреждением операционных рисков.

Базельский комитет по банковскому надзору предлагает ряд рекомендаций, касающихся национальных стандартов, принципов и лучших практических приемов надзора. Комитет надеется, что национальные

финансовые органы предпримут шаги по внедрению этих рекомендаций посредством мероприятий, предусмотренных соглашением, которые лучше всего соответствуют их национальным системам. Нормативные требования вызывают необходимость проведения аудита финансовых учреждений. Во избежание ущерба, который могут нагнести аудиты обычным бизнес-операциям, конкретные финансовые учреждения должны ввести системы (внутреннего аудита, менеджмента информационной безопасности и т.д.), предоставляющие нормативным органам все необходимое для проверки соответствия финансового учреждения всем требованиям.

Каждое финансовое учреждение должно интерпретировать «операционный риск» в показателях собственной бизнес-деятельности и определять риски, которым оно подвергается. Анализ операционных рисков должен включать в себя мошенничество и другие преступные действия, сбои системы, человеческий фактор, природные бедствия и террористические акты. Цунами, вызвавшее большие человеческие жертвы и разрушения в Азии в декабре 2004 г., и террористические атаки в сентябре 2001 г., нацеленные на индустрию финансовых услуг в городе Нью-Йорке, являются примерами событий с крайне низкой степенью вероятности. Но такие события имеют место и должны приниматься во внимание.

В [10] подчеркивается необходимость проведения учреждением систематического анализа риска. Для управления непредвиденными обстоятельствами необходимо использовать как качественные, так и количественные методы, а выбор средств контроля для индивидуальной организационной единицы должен основываться на анализе стоимости и эффективности, который рассматривает вероятность конкретного непредвиденного обстоятельства, его вероятности частоту, прогнозируемые потери и влияние на бизнес-операцию в случае наступления события.

Следует отметить различие между банковским надзором для обеспечения финансового благосостояния банков и банковским контролем, который рассматривает системы финансовых учреждений с точки зрения операционного риска. Этот контроль основан не на требованиях, установленных в [10], а на Ключевых принципах Банка международных расчетов [19], направленных на системно значимые платежные системы. Платежные системы классифицируются как «системно значимые» для благополучия и нормальных операций финансовых рынков и должны соответствовать всем десяти ключевым принципам. «Значимые системы» должны соответствовать только, по крайней мере, семи ключевым принципам. Для других платежных систем требования соответствия ключевым принципам различаются, но финансовые учреждения могут использовать свое соответствие в виде рекламного акта, так как это соответствие рассматривается как мера качества.

5.3 Разработка

После определения целей информационной безопасности организации и оценки воздействия положений и законодательства необходимо разработать план действий, согласованный с установленными бизнес-целями. План действий должен использоваться как руководство для разработки политики информационной безопасности организации (далее — политика)[1)].

Важно, чтобы организация разработала политику, которая принимает в расчет цели организации и ее конкретные аспекты. Политика должна согласовываться с бизнесом организации, культурой, нормативной и правовой обстановкой, в которых действует предприятие. Разработка политики необходима для обеспечения целесообразности и эффективности процесса менеджмента риска программы обеспечения безопасности. Для разработки и эффективного внедрения политики нужна поддержка руководства всей организации. Адаптировав политику к бизнес-целям организации, политика будет способствовать наиболее эффективному использованию ресурсов и реализует последовательный подход к обеспечению безопасности во всем спектре разных информационных систем.

5.4 Иерархия документации

5.4.1 Общий обзор

5.4.1.1 Общие положения

В настоящем стандарте приводятся три уровня документации программы обеспечения информационной безопасности. Эти три уровня состоят из документации политики, документации практических приемов обеспечения безопасности и документации операционных процедур обеспечения безопасности[2)]. Иерархия документации и значение каждого уровня показаны на рисунке 1.

[1)] В настоящем стандарте термин «политика» является синонимом термина «общая политика информационной безопасности».

[2)] Номенклатура и иерархия документации не являются фиксированными. Конкретные организации могут использовать большее число уровней иерархии и различную номенклатуру документации.

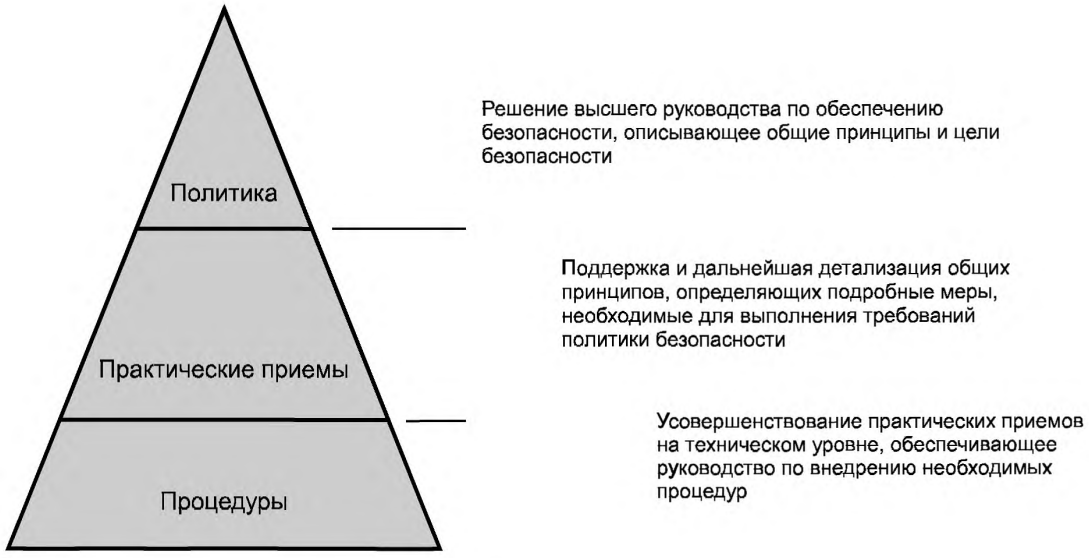


Рисунок 1 — Документация программы

В документах, относящихся к информационной безопасности, должны быть охвачены как высокоуровневые цели организации, так и конкретные, относящиеся к безопасности, настройке устройств, реализующих политику. Диапазон охвата целей лучше всего представить множественными уровнями документации. Число уровней должно быть сведено к минимуму, и настоящий стандарт рекомендует использование трех уровней: документация о политике, документация практических приемов обеспечения безопасности и документация операционных эксплуатационных процедур безопасности.

По мере внедрения в конкретной организации новой прогрессивной технологии потребуются дополнительные документы. В то время как документация политики обычно представляется на одной странице, документация процедур может состоять из нескольких многостраничных документов, представляющих отдельные специфические условия, организационные единицы и вопросы политики в организации. В некоторых случаях отдельная, вполне самостоятельная система может также иметь собственную документацию практических приемов. Все практические приемы и процедуры должны переходить с более высокого уровня на детальный уровень, поддерживая согласованность с оценками риска организации с общей политикой.

5.4.1.2 Политика информационной безопасности организации

Документ политики является наименьшим по объему из всех документов в иерархии документов программы обеспечения информационной безопасности. Обычно политика состоит из нескольких параграфов, объясняющих, что руководство рассматривает информацию в любой форме как ценный ресурс организации, который нуждается в защите. Политика должна быть широкой по масштабу и сформулированной как можно более просто и сжато и предоставлять конкретную информацию об активах, нуждающихся в защите, например данные о клиентах, сотрудниках, партнерские соглашения и процессы. Очень простой документ политика безопасности может содержать следующее единственное утверждение: «Конфиденциальность, доступность и целостность всех информационных активов организации должны быть обеспечены посредством соответствующих защитных мер».

Политика безопасности — это документ, всеобъемлющий по своему масштабу и являющийся наиболее важной частью программы информационной безопасности организации, которая влияет на ее работу. Должен существовать только единственный вариант документации политики в конкретный момент, который должен быть доведен до сведения всех сотрудников организации. Данный вариант должен быть подписан членами правления организаций, имеющими отношение к информационной безопасности, например, руководителем организации и руководителем службы информационной безопасности.

Документ политики безопасности должен быть открытым, широко распространенным и доступным всем заинтересованным сторонам организации. В документе необходимо подчеркнуть, что защита и обеспечение информационных активов являются обязанностью руководства и всех служащих и что обучение

и обеспечение осведомленности в области безопасности поручено руководству на самом высоком уровне.

Всем заинтересованным сторонам должно быть ясно, что документ политики вступает в силу при согласовании и утверждении его соответствующими должностными лицами организации. Документ должен содержать заявление о намерении организации действовать согласованно с соответствующими местными и международными правовыми и нормативными структурами и основывать свою программу информационной безопасности на твердых принципах и практических приемах, признанных в национальных и международных стандартах по безопасности.

Документ политики безопасности должен быть практически неизменным. Его изменение должно быть обусловлено изменениями стратегических целей, воспринимаемого бизнес-риска или событиями, влияющими на нормативную и правовую обстановку, в которой функционирует организация. Должностные лица организации и персонал на уровне правления должны предписывать процедуры и параметры контроля за внесением изменений.

5.4.1.3 Представительство

В разработке политики должны принимать участие представители различных видов деятельности. Группа разработки должна включать в себя членов совета директоров, административных лиц, представителей юридической службы, членов комитета по менеджменту риска и аудиторского комитета. Формулируя политику, группа разработки должна получить данные от специалистов всего предприятия, например специалистов по финансам, физической безопасности и информационным технологиям.

5.4.1.4 Классификация информации

Одним из аспектов реализации политики является классификация информации ограниченного доступа. Во многом схожие с «совершенно секретными», «секретными» и «несекретными» военными системами финансовые учреждения обладают информацией различной степени. Результаты классификации информационных активов показывают, когда следует внедрять «хорошие», «лучшие» или «наилучшие» меры управления. Существует много типов системы классификации. Важным моментом для финансового учреждения является определение классификационных уровней и использование классификации информации при вынесении решений о принятии риска. Например, риск, являющийся приемлемым для общественной информации, вероятно, будет неприемлемым для «совершенно секретной» информации. Преимущество классификации информации заключается в обеспечении поддержки руководства в отношении того, как служащие должны обращаться с информацией. Если документ, файл или база данных содержат информацию, относящуюся к различным иерархическим уровням, с ними следует обращаться в соответствии с процедурами, установленными для наивысшего классификационного уровня содержащейся в них информации.

Важно отметить, что классификационный уровень информации может меняться в течение срока ее действия. Внесение изменения должно контролироваться согласно политике организации.

5.4.2 Документы практики обеспечения безопасности

Документы практики обеспечения безопасности (далее — документы практики) основаны на содержании документации политики. Данные документы определяют общие стандарты безопасности, которым должна следовать организация. Документы практики отражают намерения и цели, установленные руководством самого высокого уровня при создании программы информационной безопасности, и документируют намерение реализовать политику независимым от технологии способом. Область действия документа практики значительно уже действия документа политики. В документ практики включают требования обеспечения безопасности организации и технологии выполнения работ по ее обеспечению. Объем документа практики является переменным и зависит от его содержания.

Число документов практики должно быть сведено к минимуму. Число необходимых документов зависит от величины организации и ее бизнес-потребностей, а также объема и сложности деятельности организации. Правовая и нормативная среды, оказывающие воздействие на организацию, могут также влиять на число необходимых документов практики.

Документ практики не является общедоступным[1)]. По своему характеру этот документ общего назначения является технологически нейтральным. Он является менее абстрактным, чем документ политики и может оказывать меньшее влияние на всю организацию, поскольку применим только к некоторым аспектам деятельности организации. Например, очень простой документ практики может содержать следующее простое утверждение: «Аутентификация доступа к информационным активам организации должна осуществ-

[1)] Возможны обстоятельства, при котором документ практики должен быть представлен регулирующим органам.

ляться в соответствии с уровнем конфиденциальности активов». Аутентификация по двум факторам представляет собой минимально приемлемый уровень аутентификации; доступ к активам, классифицированным обладателем информации как «конфиденциальные» должен осуществляться только посредством аутентификации по трем параметрам[1]. Системы управления доступом по двум факторам (биометрии и паролях) должны следовать следующим положениям...»

Полномочия документов практики основаны на политике, поэтому должны строго следовать ей, они более подвержены изменениям. Данный фактор обусловлен более частными изменениями, возникающими при идентификации новых рисков и мер управления безопасностью. Каждый документ практики имеет ограниченный круг пользователей, так как он обычно затрагивает определенную часть организации или организационной единицы и не оказывает влияния на общую программу менеджмента безопасности организации.

Целесообразно включать в документ практики обзорный раздел, в котором указывается круг пользователей и владелец каждого документа практики. Владельцем документа практики может быть управляющий делами, руководитель ИТ или руководитель группы технического сопровождения. Следует также включать в документацию сведения о том, как классифицируется информация, связанная с данными практики, так как уровень классификации указывает на уровень защиты, необходимый для информации.

5.4.3 Документы операционных процедур обеспечения безопасности

Документы операционных процедур обеспечения безопасности являются производным одного или более документов практики обеспечения безопасности. Объем этих документов зависит от темы и сложности процедур. Эти документы являются самыми краткими по своему объему из всех документов в иерархии документации. Данные документы описывают технологию реализации политики. Документы операционных процедур обеспечения безопасности относятся к реальным бизнес-системам, а определяемые поставщиком подробности о продукции приводятся в документации.

Документов операционных процедур должно быть необходимое число и при их разработке следует следить, чтобы они были полными, точными и целесообразными и не противоречили любой другой практике или политике. Примерные рекомендации, которые можно найти в любом документе операционных процедур, могут содержать следующие инструкции: «Используйте команду «pwadmin» для обеспечения соответствия паролей пользователей критериям, установленным в документации «Корпоративная практика аутентификации и управления доступом», «Дайте следующие команды...».

Документы процедур должны соответствовать общей политике организации и практическим приемам, на которых основаны эти процедуры. Документы процедур не должны противоречить основанной на политике практике. Необходимо принимать в расчет нормативные ограничения, создаваемые за пределами организаций, стандарты и другие документы процедур.

Документы процедур должны включать в себя результаты предыдущего анализа риска безопасности и проводимых руководством проверок, включая идентификацию любых остаточных рисков, результаты последующих действий (например проверки внедренных мер управления на соответствие безопасности), перечень действий, которые нужно предпринять для мониторинга и анализа информационной безопасности при повседневном использовании, и отчеты о связанных с безопасностью инцидентах.

6 Менеджмент информационной безопасности. Программа обеспечения безопасности

6.1 Общие положения

Для реализации политики требуются программы обеспечения информационной безопасности. Распоряжения руководства организации должны распространяться и подкрепляться действиями руководства более низкого уровня и персонала на высшем уровне. Обеспечение информационной безопасности является как коллективной, так и индивидуальной обязанностью. Разработка, сохранение, улучшение и мониторинг программы обеспечения информационной безопасности требуют участия большинства служб и отделов организации. Необходима тесная координация между управляющими делами и персоналом обеспечения информационной безопасности. Для поддержки программы обеспечения информационной безопасности должны использоваться такие дисциплины организации, как аудит, страхование, нормативное соответствие, физическая безопасность, обучение, кадровая и правовая дисциплины и др.

---

[1] Толкование термина «аутентификация» по трем параметрам часто выражается фразой «то, что вы имеете, то, что вы знаете, и то, чем вы являетесь». «То, что вы имеете» может быть карточкой или маркером. «То, что вы знаете» может быть пин-кодом или паролем. А для представления «того, кем вы являетесь» используются биометрические данные.

6.2 Создание программы

Наиболее важная рекомендация настоящего стандарта состоит в том, чтобы организации создавали свою программу обеспечения информационной безопасности. Эта программа должна исходить из политики, установленной для организации на высшем уровне руководства. Программа обеспечения информационной безопасности должна предусматривать разработку и поддержку детальных процессов обеспечения безопасности в масштабе организации, совместимых с политикой.

Для разработки детальных процедур и процессов обеспечения информационной безопасности может потребоваться координация различных бизнес-функций организации (включая аудит, менеджмент риска), соответствие требованиям страхования, а также координация действий работников организации, отвечающих за нормативное и правовое соответствие, партнеров и клиентов.

6.3 Осведомленность

Программа улучшения осведомленности о безопасности должна включать в себя функцию обучения и улучшения осведомленности о безопасности, гарантирующую достаточную осведомленность и бдительность всех работников в отношении своих действий и действий окружающих их людей с учетом последствий для безопасности. Программа улучшения осведомленности о безопасности должна быть структурирована для поддержания осведомленности работников о своих обязанностях, связанных с безопасностью, предоставлять ресурсы и поощрять лиц, интересующихся вопросами обеспечения безопасности с целью расширения их знаний.

6.4 Анализ

Одно или несколько должностных лиц организации должны быть назначены ответственными за программу обеспечения информационной безопасности. Установленные в программе практические приемы обеспечения информационной безопасности должны быть основанием для анализа и обновления программы, а при появлении новых угроз и уязвимостей — обеспечивать предоставление необходимых инвестиций для защитных мер. Программа должна включать в себя подробные процессы и процедуры, устанавливающие отчетность и ответственность за определение надежности программы обеспечения информационной безопасности и ее соответствие всем требованиям, и доклад об этом.

Все отчеты об анализе и мониторинге должны быть доступны руководству всех уровней, включая исполнительное руководство. Необходимо идентифицировать и документировать процедуры рассмотрения любых исключений из политики или отклонений от нее. Также должны существовать процедуры создания необходимых записей результатов аудита и записей о соответствии требованиям безопасности, а также мониторинга безопасности информации журналов аудита. Особое внимание следует уделить идентификации рисков для информации журналов аудита и требованиям, установленным для снижения этих рисков, гарантии адекватности защиты информационных активов.

6.5 Менеджмент инцидентов

Обо всех событиях информационной безопасности следует быстро сообщать, документировать их и разрешать их в соответствии с практическими приемами организации. Если нежелательные или неожиданные события информационной безопасности имеют высокий показатель вероятности компрометации бизнес-операций и создания угрозы для информационной безопасности, они становятся инцидентами информационной безопасности, подлежащими изучению. Как инциденты, так и события информационной безопасности должны использоваться специалистами в сфере безопасности при повторной оценке ими риска и выборе и внедрении мер управления безопасностью. События и инциденты должны использоваться при последующем улучшении программы обеспечения информационной безопасности.

6.6 Мониторинг

Необходимо создать формальные процессы оповещения о вторжениях, неправильном срабатывании систем и других инцидентах безопасности, а также о результатах расследования инцидентов безопасности. Результаты документирования менеджмента инцидентов должны использоваться в процессе анализа с целью оказания влияния на разработку защитных мер, а также инициирования переоценки и изменения с течением времени мер управления, используемых для обеспечения защиты активов.

6.7 Соответствие требованиям

Независимый анализ должен обеспечивать соответствие практических приемов организации установленной политике и адекватность и эффективность мер управления. Все разрешенные отступления от политики для проведения их периодических переоценок должны документироваться и ограничиваться во времени.

6.8 Поддержка

Все установленные защитные средства, такие, как межсетевые экраны и программные средства обнаружения вирусов, должны регулярно обновляться с целью поддержания их эффективности в отношении новых возникающих угроз.

6.9 Восстановление после любых прерываний деятельности организации

Программа обеспечения информационной безопасности должна определять информационные активы, являющиеся критичными для продолжения ведения деятельности (бизнеса) организации в случае ее (его) прерывания. Программа должна создавать подробные письменные планы возобновления деятельности (бизнеса) после ее (его) прерывания. Для выполнения программы обеспечения информационной безопасности необходимо использовать квалифицированный персонал, правовые соглашения (договоры), системы резервирования информации, ресурсы обработки и специальные помещения, в которых поддерживается критическая деятельность организации. Планы восстановления деятельности (бизнеса) организации после прерывания должны регулярно тестироваться и оцениваться.

7 Структура информационной безопасности

7.1 Приверженность целям организации

Выполнение целей программы обеспечения информационной безопасности в масштабе организации должно основываться на понимании как глобальных, так и внутренних потребностей информационной безопасности организации. Организация должна демонстрировать приверженность программе обеспечения информационной безопасности посредством своей готовности выделять ресурсы для мероприятий, связанных с информационной безопасностью, и изучать потребности информационной безопасности. На самом высоком уровне необходимо осознание значения информационной безопасности для организации, а также ее масштаба и объема деятельности.

Все работники организации должны знать цели информационной безопасности. Каждый служащий или подрядчик должен осознавать свои роль и обязанности, а также свой вклад в обеспечение информационной безопасности и обладать полномочиями для достижения этих целей.

7.2 Структура организации

7.2.1 Роли и обязанности

Назначение программы обеспечения информационной безопасности заключается в обеспечении конфиденциальности, целостности и доступности информационных активов путем комплексного решения сформированных целей и задач безопасности в программе. Соответствующее назначение и разграничение обязанностей должно быть связано с определенными ролями (функциями деятельности). Процедуры обеспечения информационной безопасности должны обеспечивать эффективное выполнение и осуществление всех важных задач.

7.2.2 Совет директоров

Совет директоров финансовых учреждений должен иметь обязательства перед организацией и ее членами по осуществлению надзора за практическими приемами менеджмента бизнес-деятельности организации. Эффективные практические приемы обеспечения информационной безопасности должны входить в целесообразную бизнес-практику и демонстрировать заинтересованность в формировании общественного доверия. Совет директоров должен пропагандировать важность информационной безопасности и поддерживать программу обеспечения информационной безопасности.

7.2.3 Комитет по аудиту

Комитет по аудиту в финансовом учреждении должен оказывать содействие совету директоров в осуществлении надзора и служить независимым органом проведения объективного анализа, основанного на внутренних мерах защиты и финансовой отчетности. Мониторинг и тестирование внутренних защитных мер, являющихся частью программы обеспечения информационной безопасности, входят в обязанности комитета по аудиту, обычно осуществляемые посредством внутреннего аудита организации и внешних аудиторов.

7.2.4 Комитет по менеджменту риска

Комитет по менеджменту риска, подчиняющийся совету директоров, должен анализировать программу обеспечения безопасности и поддерживать финансирование проектов обеспечения информационной безопасности в том случае, когда эти проекты снижают операционный риск (и, следовательно, финансовый риск) организации. Комитет по менеджменту риска должен демонстрировать приверженность организации обеспечению безопасности путем финансирования и поддержки проектов, способствующих осуществлению политики информационной безопасности организации. Комитет по менеджменту риска должен определять степень воздействия на программу обеспечения информационной безопасности положений и законодательств. Этот аспект см. 5.2.

7.2.5 Правовая функция

Организации могут полагаться на опыт своего юридического отдела в отношении некоторых аспектов менеджмента информационной безопасности. Юридическому отделу может быть вменено в обязанность осуществление мониторинга поправок в законодательстве, постановлениях и судебных делах, которые могут влиять на программу обеспечения информационной безопасности организации.

От юридического отдела может потребоваться проверка контрактов, касающихся служащих, клиентов, провайдеров услуг, подрядчиков и поставщиков с тем, чтобы гарантировать адекватное рассмотрение связанных с информационной безопасностью юридических проблем. Такие проверки могут включать в себя вопросы неприкосновенности частной жизни или техники безопасности на рабочем месте, а также процедуры увольнения и рассмотрения жалоб служащих.

При рассмотрении правовых аспектов инцидентов безопасности и их влияния на организацию могут потребоваться консультации юридического отдела. Организации могут затребовать экспертные заключения при оценке последствий процедур урегулирования инцидентов безопасности и обеспечения их соответствия правовым требованиям среды функционирования, так как в соответствии с юридическим статусом организации правовые нормы могут иметь различия. Необходимо вовлекать юридический отдел в разработку, поддержание и улучшение процедур обработки последствий инцидентов безопасности, таких как сохранение свидетельств.

7.2.6 Должностные лица

Руководитель организации или управляющий как самое главное должностное лицо в организации несет всю полноту ответственности за ее функционирование. Руководитель организации должен санкционировать создание программы обеспечения информационной безопасности в соответствии с действующими нормативно-правовыми документами и стандартами, оказывать поддержку в ее осуществлении, следить за выполнением важных решений, связанных с оценкой риска, и участвовать в пропаганде значимости обеспечения информационной безопасности.

В то время как во многих организациях имеются должности руководителя организации, финансовой службы организации, технического отдела и административной службы, многие организации стали вводить также дополнительные должности руководителя по информационным технологиям и руководителя службы обеспечения информационной безопасности на верхнем уровне структуры организации. Хотя руководитель технического отдела, руководитель по информационным технологиям и службы обеспечения информационной безопасности выполняют много взаимозаменяемых функций, каждое финансовое учреждение должно также иметь руководителя службы обеспечения информационной безопасности, который, в конечном счете, должен быть подотчетен руководителю технического отдела или руководителю по информационным технологиям.

7.2.7 Управляющие делами

Управляющие делами в частности и управляющие всей организации в целом должны осуществлять надзор и мониторинг деятельности организации и ее работников, что делает их ключевыми участниками программ обеспечения информационной безопасности. Каждый управляющий должен понимать и поддерживать политику, практические приемы и процедуры организации, следовать им, а также обеспечивать соответствующее поведение служащих, поставщиков и подрядчиков. Управляющие делами должны создавать в организации атмосферу, поощряющую служащих, поставщиков и подрядчиков сообщать о проблемах, связанных с информационной безопасностью.

7.2.8 Сотрудники

Требования программы обеспечения безопасности должны быть включены в контракты о найме служащих. Весь персонал должен быть осведомлен о последствиях своих действий и действий окружающих в отношении безопасности. Служащие должны незамедлительно сообщать обо всех подозрительных событиях, связанных с информационной безопасностью.

7.2.9 Сотрудники (персонал), не относящиеся к организации

Требования программы обеспечения безопасности должны быть включены в соглашения с подрядчиками и поставщиками услуг. Подрядчики и поставщики услуг должны быть осведомлены о практических приемах и процедурах обеспечения информационной безопасности организации и ее подразделений и оказывать им поддержку. Они обязаны соблюдать политику информационной безопасности организации. Так как по экономическим или иным причинам организации могут предпочесть привлечение внешних ресурсов для выполнения определенных банковских функций, менеджмент риска не может быть передан сторонним организациям и должен оставаться под ответственностью организации.

7.2.10 Должности, связанные с безопасностью

7.2.10.1 Введение

В настоящем пункте определяются три связанные с безопасностью должности в рамках программы обеспечения информационной безопасности, которые наделяются разными уровнями обязанностей и функциями, необходимыми для выполнения программы обеспечения информационной безопасности. Данные должности функционально определены, хотя способы административного управления персоналом организации могут различаться.

В некоторых организациях отвечающей за информационную безопасность персонал может представлять собой отдельную структурную единицу, а в других организациях персоналу функциональных структур (отделов, служб) могут быть поручены обязанности, связанные с обеспечением информационной безопасности в дополнение к собственным. Возможно также совмещение двух обязанностей.

Какую бы структуру не имела программа обеспечения информационной безопасности, должностные лица и управляющие должны оказывать данной программе поддержку для повышения ее эффективности. В больших организациях может быть полезно создать дополнительные должности для эффективного выполнения специализированных функций, например, разработчик архитектуры безопасности. В более мелких организациях персоналу, вероятно, придется выполнять несколько обязанностей одновременно.

7.2.10.2 Руководитель службы обеспечения информационной безопасности

Руководитель службы обеспечения информационной безопасности отвечает за проектирование, внедрение программы обеспечения информационной безопасности и управлению ею. Под управлением руководителя службы обеспечения информационной безопасности персонал на других уровнях выполняет обязанности по осуществлению политики и практических приемов программы обеспечения информационной безопасности. Руководитель службы обеспечения информационной безопасности может иметь специальный штат и осуществлять административное управление персоналом, отвечающим за информационную безопасность. Также руководитель службы обеспечения информационной безопасности может осуществлять ограниченный оперативный контроль за персоналом, выполняющим обязанности, связанные с информационной безопасностью, в дополнение к своим основным обязанностям. Независимо от величины организации или стиля руководства, руководитель службы обеспечения информационной безопасности является лицом, несущим всю ответственность перед советом директоров и управляющими за выполнение программы обеспечения информационной безопасности.

Руководитель службы обеспечения информационной безопасности должен управлять выполнением программы обеспечения информационной безопасности в соответствии с условиями, определенными организацией как необходимые для успеха в бизнесе. Руководитель службы обеспечения информационной безопасности отвечает за:

- подготовку финансовой сметы и обоснование программы обеспечения информационной безопасности перед управляющими;
- разработку архитектуры безопасности, которая согласуется со стратегией бизнеса;
- руководство персоналом разных уровней, который внедряет архитектуру безопасности и выполняет связанные с обеспечением информационной безопасности обязанности;
- проведение оценок риска, которые подтверждают правильность архитектуры безопасности, и раскрытие недостатков, требующих особого внимания;
- придание огласке политики, практических приемов и процедур обеспечения безопасности и управление программы повышения осведомленности о безопасности;
- осведомленность о текущих угрозах и уязвимости, а также новых методах и средствах обеспечения информационной безопасности для противодействия этим угрозам и уязвимостям;
- обеспечение соответствующего вовлечения организации в деятельность по защите критической инфраструктуры в странах, где организация ведет свой бизнес.

7.2.10.3 Ответственный за информационную безопасность

Ответственный за информационную безопасность — это любое лицо в организации, отвечающее за разработку, внедрение и поддержку программы обеспечения информационной безопасности под руководством руководителя службы обеспечения информационной безопасности. Лица, ответственные за информационную безопасность, могут входить в штат руководителя службы обеспечения информационной безопасности или быть внештатными сотрудниками, находясь в административном подчинении в другом структурном подразделении организации. Ответственный за информационную безопасность, имея обширные знания и опыт, может быть назначен на особую должность, например на должность разработчика архитектуры безопасности. Сотрудники, ответственные за информационную безопасность, могут обладать специализированными значениями в области таких методов и средств обеспечения информационной безопасно-

ти, как оценка риска, осведомленность об угрозах и т. д., и являться важным потенциалом для организации. Другие ответственные за информационную безопасность лица должны консультировать и давать рекомендации организационным единицам по проблемам информационной безопасности. Деятельность ответственных за информационную безопасность будет наиболее эффективной, если они знают бизнес-цели, а также внутренние процессы организации.

Ответственные за информационную безопасность должны:

- знать архитектуру, практические приемы и процедуры безопасности;
- разрабатывать локальные практические приемы, доводить до сотрудников организации и обновлять их при необходимости;
- проводить оценки риска;
- осуществлять мониторинг и аудит практических приемов обеспечения безопасности;
- содействовать восстановлению системы ИТ после атак;
- давать рекомендации по улучшению практических приемов и процедур;
- быть в курсе развития угроз информационной безопасности, технологий, а также методов и средств обеспечения информационной безопасности;
- способствовать осведомленности руководства и сотрудников службы безопасности в информационной безопасности.

7.2.10.4 Операторы обеспечения безопасности

Операторы обеспечения безопасности выполняют подробные действия для достижения целей программы обеспечения информационной безопасности. Операторы обеспечения безопасности могут состоять в штате руководителя службы обеспечения информационной безопасности или административно относиться к другим подразделениям организации и должны быть хорошо осведомлены об аппаратных и программных средствах и процедурах безопасности, необходимых для своих подразделений.

Из-за разнообразия технологий, которые могут использоваться в архитектуре безопасности, от операторов обеспечения безопасности требуется выполнение многих процедур. Некоторые специфические обязанности, возлагаемые на операторов безопасности, включают в себя:

- установку и сохранение связанных с безопасностью настроек на сетевом оборудовании;
- установку обновленных версий защиты в операционные системы;
- сохранение и модернизацию точных файлов управления доступом;
- сбор информации, относящейся к информационной безопасности, и информации об аудите, а также мониторинг системной и сетевой деятельности с целью обнаружения связанных с безопасностью проблем.

Широкое разнообразие выполняемых задач определяет значимость операторов обеспечения безопасности в успешном функционирования программы обеспечения информационной безопасности.

Операторы обеспечения безопасности отвечают за:

- знание своей роли в выполнении программы и архитектуры обеспечения безопасности;
- внедрение и поддержание практических приемов и процедур безопасности;
- мониторинг процедур безопасности и сообщение об их состоянии исходя из обстановки;
- работу над исправлением сбоев в обеспечении безопасности и противодействием атакам;
- восстановление соответствующих процедур безопасности во взаимодействии с восстановлением бизнес-процесса после сбоя или атаки;
- предоставление рекомендаций по улучшению практических приемов и процедур.

8 Анализ и оценка риска

8.1 Процессы

Организации, желающие получить доступ к информации о состоянии своих дел по безопасности, должны внедрить один или несколько процессов анализа риска как часть программы обеспечения информационной безопасности. Эти процессы должны использоваться для оценки состояния безопасности всей организации, а также безопасности конкретных проектов, систем и продуктов. Поскольку стили руководства, масштаб и структура организаций различаются, могут потребоваться несколько стратегий для адаптации анализа риска к среде, в которой риск используется[1)].

Результатом процесса оценки риска должны быть рекомендации по снижению рисков безопасности организации до приемлемого уровня. Данные рекомендации должны способствовать выбору соответству-

[1)] Дополнительную информацию можно найти в [2], [5], [20], [21].

ющих защитных мер. Защитные меры являются результатом оценки и определения величины возможных потерь, которые могут произойти в случае использования идентифицированных уязвимостей системы одной или более угрозами. К активам организации, которые обычно подвергаются оценке риска, относят: аппаратуру и оборудование, прикладные программы, базы данных организации, системы связи и компьютерные операционные системы.

Примеры метода проведения оценок риска и типичного процесса оценки риска приведены в приложении С. Дополнительные модели оценки риска представлены в [2], [5], [20], [21]. Дополнительные модели в качестве примера также приведены в приложении С и не предполагают их использования организацией непосредственно в качестве технологических карт внедрения.

8.2 Процесс оценки риска

Финансовые и другие организации испытывают влияние рисков, связанные с их бизнесом. Риски, относящиеся к информационным активам организации, принимают различные формы и должны подвергаться тщательному анализу. Оценки риска нужны при изучении уязвимостей, угроз и рисков для информации. Каждое банковское приложение должно обеспечивать контекст и знание рабочих процессов, а также потенциальные угрозы и зоны уязвимости. Данное знание имеет значение для проведения оценки риска. Оценка риска представляет собой трехступенчатый процесс:

Первая ступень — оценка рисков потенциальных угроз для каждой зоны уязвимости путем заполнения таблицы оценки риска (см. приложение С);

Вторая ступень — присвоение комбинированного уровня риска каждой зоне уязвимости путем заполнения таблицы оценки риска (см. приложение С);

Третья ступень — определение подходящих политик безопасности и защитных мер, используя результаты второй ступени и имеющиеся меры управления.

Более подробный список категорий риска и их применение в процессе оценки риска представлены в приложении С.

8.3 Рекомендации по обеспечению безопасности и принятие риска

Оценка риска может проводиться:

- для оценивания риска на уровне организации;
- в рамках взаимосвязанной совокупности систем;
- для отдельной системы или приложений;
- для конкретных критических функций внутри системы.

Не следует ожидать, что оценка риска на уровне организации является только комбинацией всех критических функций организации.

Уязвимости и угрозы постоянно меняются по мере появления новых технологий обнаружения уязвимостей в системах, введения новых или модернизированных продуктов, определяемых ростом и развитием организации. Поэтому степень детализации и выводы оценки риска для разных систем могут сильно различаться в рамках организации и для сходных систем в разных организациях.

Тем не менее любая оценка риска должна завершаться формированием набора рекомендаций по обеспечению информационной безопасности оцененной системы. В наборе рекомендаций риски, связанные с системой, рассматриваются как реализованные. В обязанность управляющих делами входит принятие этих рисков. Во многих случаях допускается применять дополнительные меры управления (или они могут быть применены на этапе проектирования или разработки) для снижения рисков до более приемлемого уровня. Принятие рисков должно регулироваться практическими приемами обеспечения безопасности организации. При рассмотрении исключений из политики управляющий делами должен работать над гарантированием соответствия политике в будущем или принятием долговременной исключительной ситуации как остаточного риска вместе с группой по обеспечению информационной безопасности.

9 Выбор и внедрение защитных мер

9.1 Снижение риска

Любая система обладает уязвимостями, посредством которых нарушители могут угрожать организации финансовыми убытками, падением продуктивности или утратой престижа. Минимизация и ослабление этих рисков является общей обязанностью управляющих делами и группы по обеспечению информационной безопасности, работающих вместе с другими группами в финансовом учреждении. Существует много аспектов менеджмента риска, и наиболее значимые уже обсуждались, например, приверженность высшего руководства к обеспечению информационной безопасности; ответственность руководителя службы обеспечения информационной безопасности, отвечающего за внедрение и управление программой обеспечения безопасности, и в целом за программу обеспечения безопасности.

Значимые процессы и технологии, обычно используемые или учитываемые для ослабления риска, приведены в 9.2—9.7. Данные процессы и технологии могут использоваться во время процесса разработки, после оценки слишком высокого риска или идентификации новой уязвимости. Управляющие делами должны помнить о преимуществах документирования встраиваемой системы безопасности вместо попыток произвольного исправления имеющихся нарушений безопасности системы.

Использование данных технологий может обеспечить непосредственное управление рисками, которое организация берет на себя. Организация должна оценить, как запланированные и существующие меры управления снижают риски, идентифицированные при анализе риска, определить дополнительные меры защиты, которые имеются или могут быть разработаны, спроектировать архитектуру информационной безопасности и определить ограничения различных типов. Затем необходимо выбрать адекватные и обоснованные меры управления для снижения оцененных рисков до приемлемого уровня остаточного риска. Дополнительные подробности, касающиеся выбора мер управления, см. в [2], [5], [20], [21].

9.2 Идентификация и анализ ограничений

На выбор мер управления могут оказать влияние многие ограничения. Эти ограничения следует принимать в расчет при составлении рекомендаций и во время внедрения. Ограничения и соображения приведены в таблице 1.

Таблица 1 — Характеристики ограничений и соображений

Ограничения	Примечание
Временные	Меры управления должны быть внедрены за период времени, приемлемый для руководства, в течение срока службы системы и должны оставаться эффективными, насколько руководство считает необходимым
Финансовые	Внедрение мер управления не должно быть дороже, чем ценность активов, которые они предназначены защищать
Технические	Меры управления должны быть технически осуществимыми и совместимыми с системой
Социологические	Меры управления могут быть специфическими для страны, отрасли, организации или даже отдела организации для обеспечения доступности для персонала
Связанные с окружающей средой	Выбранные меры управления должны быть приспособлены к территории, климатическим и природным условиям и расположению населенного пункта
Нормативные	Меры управления должны соответствовать нормативным правовым требованиям, например, защите персональных данных или не специфичным для ИТ нормам из уголовного кодекса, правилам из инструкций по пожарной безопасности, трудового кодекса и т. д.

9.3 Логический контроль доступа

9.3.1 Общие положения

Логический контроль доступа относится к техническим методам и мерам управления, используемым в системах и приложениях для ограничения доступа к информации в соответствии с практическими приемами организации. В основном пользователям должен предоставляться минимальный доступ, необходимый для выполнения их рабочих функций, но часто ограниченность системы, конструктивные или другие ограничения могут приводить к тому, что пользователи имеют дополнительный доступ. Тем не менее пользователю необходима регистрация доступа к системе, то есть фиксация того, кому предоставляется право доступа, какие сотрудники имеют доступ, когда он осуществлялся. Наиболее важной функцией является необходимость соблюдения определенных ограничений доступа. Меры управления для осуществления эффективного контроля доступа приведены ниже.

9.3.2 Идентификация пользователя

У многих пользователей должна быть причина для получения доступа к информации и информационным системам финансового учреждения. Такими пользователями являются служащие, клиенты, системные администраторы и управляющие. В большинстве случаев необходимо с некоторой степенью определенности знать, какая категория пользователей пытается получить доступ к определенному приложению. Очень часто необходимо знать не только категорию, но также личность того, кто пытается получить доступ.

Традиционно каждая информационная система имеет собственный процесс идентификации пользователя. Из-за быстрого расширения систем появилась необходимость в процессе идентификации, общем для всех и удовлетворяющим многие системы. Может также потребоваться для услуг по идентификации привлечение внешних ресурсов. Приведенные ниже рекомендации должны применяться независимо от того, кто предоставляет услуги по идентификации.

Для обеспечения большей уверенности в тождестве личности пользователя организация должна создавать и осуществлять политику, требующую подтверждения личности пользователя перед выдачей идентификатора пользователя. Целесообразная бизнес-практика требует интегрирования требований «знай своего клиента» и «знай своих служащих» в мероприятия по выдаче идентификатора пользователя. Более того, организация должна выполнять процедуры выдачи идентификатора и контролировать их для гарантии того, что каждый идентификатор нового пользователя являлся уникальным и может быть отслежен до идентифицированного сотрудника и сотрудника, выдавшего идентификатор.

9.3.3 Санкционирование

Санкционирование является действием по предоставлению пользователю возможности выполнения конкретных действий в системе на основе аутентификации его личности. Организация должна определить права доступа каждого пользователя. Без специальной санкции ни одному пользователю не разрешается доступ к какой-либо информации или приложению.

Существует несколько принципов сохранения записей средств контроля доступа, основанных на ролях (должностях). Одним из традиционных принципов является поддержка централизованного списка привилегий для каждого пользователя. Администраторы безопасности информационных систем, обычно работающие под двойным контролем, отслеживают и сохраняют такие записи. Программные средства защиты данных должны сопоставлять идентификатор пользователя с записями и разрешать пользователям доступ к информации или приложениям в соответствии с записями.

Другой принцип предназначен для распределенного сохранения записей с листингом управления доступом по каждой системе или отдельным доступом для различных видов приложений (например «тонкий» клиент, «толстый» клиент, сеть, многозвенное приложение, веб-сервесы и т. д.).

9.3.4 Аутентификация пользователей

9.3.4.1 Механизмы аутентификации

Аутентификация пользователей относится к процессу (например, процедурному, физическому или выполняемому с помощью аппаратных/программных средств), посредством которого идентификатор пользователя проверяется системой. Пользователи могут принадлежать к организации или внешним организациям, и неспособность аутентифицировать личность пользователя снижает возможность данной организации обеспечить подотчетность действий отдельного лица и может допустить несанкционированный доступ к данным и компьютерным ресурсам.

Существует несколько типов механизмов аутентификации. Их действие основывается на одной или нескольких следующих характеристиках:

- что-то, что пользователь знает (например пароли);
- нечто, известное пользователю (например смарт-карта);
- какие-либо физические характеристики пользователя (например отпечатки пальцев или другие биометрические данные). Комбинация разнообразных механизмов аутентификации может обеспечить более высокий уровень аутентификации.

9.3.4.2 Цифровые сертификаты

Цифровые сертификаты могут использоваться для подписания или шифрования информации и обеспечения аутентификации пользователя, кода программы или устройства. Цифровые подписи, основанные на сертификатах, могут использоваться для аутентификации источника информации, целостности данных и услуг по обеспечению свойства неотказуемости. Основанные на сертификатах услуги по защите данных могут быть предоставлены с помощью шифрования. Меры управления и синтаксис, необходимый для управления сертификатами X.509 в сфере финансовых услуг, определены в [3]. Подробная информация об управлении информацией о политике безопасности сертификатов в организации и необходимых элементах формулировок практики, связанной с сертификатами, предоставлена в ИСО 21188 [22].

9.3.4.3 Пароли

В настоящее время наиболее распространенным методом аутентификации являются пароли. Пароль представляет собой строку символов, составленную из любой комбинации букв, цифр и специальных символов клавиатуры. Знание пароля, ассоциирующегося с пользователем, является подтверждением санкционирования использования возможностей, связанных с этим пользователем (например доступ к определенным программам, возможностям и файлам системы).

Пароли могут быть динамическими (например, генерируемые и изменяемые автоматически и, часто, программными средствами) либо статическими (например, редко изменяемые по усмотрению пользователя). Рекомендации по формированию и контролю за использованием паролей можно найти во многих публикациях и в сети. Например «Рекомендации по управлению паролями Министерства обороны США» от 12 апреля 1985 г. (CSC-STD-002-85) [23] предоставляют техническую трактовку генерации, контроля и использования паролей в организации. Обсуждение на сайте gost.e-ecolog.ru password.htm [24] предоставляет более общую трактовку темы об использовании паролей и включает в себя дискуссию о составе и длине, изменении, хранении паролей и их совместном использовании.

9.3.4.4 Биометрия

Биометрия является методом идентификации людей по некоторым физическим характеристикам, которые могут быть измерены и с высокой степенью вероятности являются уникальными для человека. Отпечатки пальцев являются наиболее известными биометрическими данными. Существуют электронные устройства, способные считывать отпечаток пальца и сравнивать его с отпечатком, уже хранящимся в системе. Другие физические характеристики, которые могут быть использованы в биометрической системе идентификации, включают в себя узор сетчатки глаза, геометрию ладони, черты лица и голос.

Способы осуществления менеджмента биометрической информации в сфере финансовых услуг в качестве части программы менеджмента информационной безопасности организации представлены в ИСО 19092 [25]. Настоящий стандарт устанавливает цели контроля, меры управления и подробные требования к журналу регистрации событий управления биометрической информацией и результатов контроля.

9.4 Журнал аудита

Журнал аудита представляет собой журнал, создаваемый системой записи осуществленной деятельности, используемый организацией как средство восстановления событий и ведения подотчетности. Информация, содержащаяся в журнале аудита, необходима для разрешения проблем или споров, а также для предоставления свидетельств о соответствии требованиям информационной безопасности. Журнал аудита способствует ограничению несанкционированной деятельности, и обеспечивает раннее обнаружение подобной деятельности. Все системы записи должны обеспечивать определенную степень детализации журнала аудита в соответствии с политикой организации. Более того, уровень детализации должен быть как можно более высоким и согласовываться с практическими потребностями и политикой организации. По возможности, регистрация в журнале аудита должна обеспечивать предупреждение ответственного лица в режиме реального времени о важных событиях, связанных с безопасностью.

Система аудита должна сообщать о любой подозрительной деятельности содействия ограничению и обнаружению несанкционированной деятельности и способствовать их быстрому расследованию. Анализ информации журнала аудита должен проводиться регулярно (обычно ежедневно) руководством, и все исключительные и необычные ситуации, связанные с безопасностью, должны расследоваться и оформляться в виде отчета.

Информация журнала аудита должна храниться в течение периода времени, соответствующего требованиям бизнеса. Информация должна быть защищена от случайного или преднамеренного удаления, модификации или фальсификации.

9.5 Контроль за внесением изменений

Для защиты целостности средств обработки информации организации необходимо внедрять процедуры контроля за внесением изменений. Отсутствие такого контроля может привести к финансовым убыткам или падению продуктивности из-за неправильных технологических процессов или невыполненного обслуживания. Для изменений аппаратных средств, изменений средств программирования, включая приложения и управление патчами для операционных систем, а также изменений неавтоматизированных процедур, должны существовать процедуры контроля таких изменений. Процедуры контроля после внесения изменений должны также включать в себя управление такими изменениями в чрезвычайных ситуациях.

Управляющие делами должны обеспечивать надлежащие процессы контроля за внесением изменений в системы, находящиеся под их управлением. Группа обеспечения информационной безопасности должна быть готова к оказанию помощи в управлении связанных с безопасностью изменениями и изменениями систем безопасности, за управление которыми непосредственно отвечает группа информационной безопасности.

9.6 Осведомленность об информационной безопасности

Частью программы обеспечения информационной безопасности должна быть программа по повышению осведомленности о безопасности с целью обучения служащих организации мерам защиты ценной информации. Программа предназначена оказывать позитивное влияние на отношение сотрудников к информационной безопасности. Повышение осведомленности сотрудников о безопасности должно осуществляться постоянно.

Программа повышения осведомленности о безопасности должна предусматривать ознакомительный курс для новых сотрудников и сотрудников другой организации. В случае введения новых приложений или внесения значительных изменений в существующие приложения в данную программу целесообразно проводить обучение сотрудников. Данной программой также должно быть предусмотрено постоянное изучение проблем безопасности, появляющихся в прессе.

Для различных уровней управления и кадровой структуры характерны разные проблемы безопасности. При обращении к каждому уровню необходимо учитывать их конкретные проблемы. Проблемы должны быть в такой форме представлены, чтобы работники всех уровней и с различными навыками смогли их понять. Управляющие делами должны быть осведомлены о внешних воздействиях, рисках и потенциале потерь, а также нормативных требованиях к информационной безопасности и требованиях аудита. Условие по осведомленности должно соблюдаться как в условиях бизнес-деятельности, так и в сфере ответственности управляющего делами.

9.7 Человеческий фактор

Сотрудники представляют собой один из наиболее важных активов финансового учреждения. Заинтересованность и взаимодействие сотрудников очень важны для успешной реализации программы обеспечения информационной безопасности. Благодаря возросшей осведомленности о безопасности сотрудники станут более внимательны и смогут замечать отклонения от выполнения норм информационной безопасности в технологических процессах или операционных процедурах организации, которые могут указывать на возникновение проблемы безопасности.

С другой стороны, сотрудники могут совершать ошибки, неправильно использовать технологию, совершать преступные действия, что создает необходимость в переговорах руководителя службы обеспечения информационной безопасности со всеми отделами организации при разработке программы обеспечения информационной безопасности и повышения осведомленности сотрудников. Другие отделы могут вносить свой вклад в виде представления мнения о сотрудниках организации с целью минимизации вероятности ошибок и предотвращения криминальной деятельности.

Некоторые должности в организации могут быть регламентированы как «доверенные», так как эти должности дают право разрешать или запрашивать доступ к конфиденциальной кадровой или финансовой информации. Другую доверенную должность может занимать сотрудник, имеющий широкие полномочия или возможности, связанные с компьютерами или активами ИТ организации. Сотрудник, выбираемый на «доверенные» должности, должен отличаться высокой честностью и проходить проверку биографии. Сотрудники, занимающие доверенные должности, должны быть осведомлены о необходимости ограничения обсуждения с семьей и знакомыми конфиденциальных подробностей о бизнесе. Конкуренты по бизнесу могут пытаться прибегнуть к социотехнике или подстрекательству человека к раскрытию информации несанкционированным лицам, а также использовать ложный интерес человека к работе, технические дискуссии и лесть, чтобы побудить служащего нечаянно раскрыть конфиденциальную информацию.

10 Меры защиты систем информационных технологий

10.1 Защита систем информационных технологий

Существует много способов обеспечения защиты систем ИТ. Меры защиты систем ИТ могут включать в себя политику организации. Однако, учитывая вопросы рассматриваемого раздела, меры управления и защиты систем ИТ будут представлены настройками системы и внешними мерами противодействия (например шифрование), которые могут использоваться для обеспечения аутентификации, санкционирования, конфиденциальности, целостности, доступности и других услуг безопасности. Применяемые в настоящее время меры противодействия и управления будут также обсуждены и в будущем.

В дополнение к первоначальному размещению мер управления и противодействия внешним воздействиям организация должна предпринять шаги для обеспечения их долгосрочного функционирования и поддержки. Иначе с течением времени, когда будут известны новые уязвимости, а установленные патчи — проигнорированы, безопасность системы ухудшится. Эффективно действующая программа обеспечения безопасности должна включать в себя процессы и процедуры поддержки, обеспечивающие наличие необходимых мер управления и защиты и их постоянное обновление.

10.2 Защитные меры аппаратных систем

Защита аппаратных систем в среде ИТ является решающей предпосылкой для поддержания целостности информационных активов. Некоторые из наиболее важных мер управления защитой критических ресурсов приведены в приложении D. Настоящий стандарт не содержит попытки включить в него список всех ресурсов ИТ, которые может использовать организация, а скорее содержит краткое обсуждение

каждого из нескольких главных типов ресурсов, а также некоторые меры управления, которые могут использоваться для предотвращения угроз этим ресурсам (см. приложение D, раздел D.1). Каждое обсуждение должно происходить по одной схеме и рассматривать ключевые вопросы, включающие в себя изучение следующих аспектов:

- почему та или иная система является важной;
- какие зоны безопасности могут быть наиболее важными;
- какие меры управления должны быть рассмотрены.

Одной из проблем, которой не уделяется должного внимания и которую организации иногда вообще игнорируют, является проблема производителей (поставщиков) аппаратных систем. Обычно принимается на веру, что производители (поставщики) оборудования действуют по поручению финансового учреждения и достаточно осведомлены о целях и политике безопасности. Однако есть вероятность, что аппаратные средства, поставляемые производителем или торговым посредником, могут быть сконфигурированы на предоставление несанкционированного доступа к информации или сетевым соединениям. Произвольное приобретение и случайное распределение аппаратных средств в сети могут содействовать защите от этого вида преднамеренной или непреднамеренной угрозы безопасности. Для применения аппаратных средств, требующих высокой степени безопасности, возможно следует рассмотреть меры управления, укрепляющие доверие между организацией и поставщиком.

Проведение оценки аппаратных средств в соответствии с FIPS 140-2[1)] [26] считается необходимым, в особенности в отношении криптографических устройств. Для других устройств при выборе и использовании прибора следует полагаться на оценки по соответствующим общепринятым критериям или специализированным профилям защиты.

10.3 Безопасность систем программного обеспечения

Поскольку современные финансовые учреждения полагаются на автоматизацию при обработке практически всех своих бизнес-операций, в основу программы обеспечения информационной безопасности должно быть положено обеспечение безопасности совокупности программ на носителях данных и программных документов, предназначенных для отладки, функционирования и проверки работоспособности автоматизированных систем [далее — программное обеспечение (ПО)]. Обеспечение безопасности систем ПО затруднено вследствие его сложности, множества его взаимодействий и разнообразных способов доступа к различным программам. Многие программы, подобные межсетевым экранам, веб-серверам и серверам приложений, предназначены для работы на многих аппаратных платформах. Безопасность систем ПО на высоком уровне рассматривается в приложении А, раздел А.2. Кроме того, существует большое число работ, в которых подробно обсуждается вопрос обеспечения безопасности программ различных типов.

10.4 Меры защиты сетей и сетевых систем

Хотя часто считается наиболее критичным вычислительный комплекс организации, включающий в себя конечные системы и различные виды серверов, большая часть трафика между системами проходит через сеть, которая не шифруется и не защищается. Значительная часть Интернета и специализированные линии многих компаний используют одинаковые открытые протоколы, системы маршрутизации и в некоторых случаях используют одни и те же сетевые устройства и коммутаторы с трафиком других компаний.

Сетевой трафик уязвим к внешним атакам, связанным с изменением маршрутизации, копированием и сетевым «анализатором пакетов»[2)], которые легко могут пройти полностью необнаруженными сетью и системами, использующими сеть и системы. Хотя шифрование часто рассматривается в качестве основного решения проблемы обеспечения безопасности, шифрование сетевого уровня может быть слишком дорогостоящим с точки зрения эксплуатации, пропускной способности и создания задержки информации для многих организаций. Даже в случае использования протоколов SSL, IPSEC и других протоколов безопасности связи, они не обязательно являются первым этапом обеспечения защиты сетевой безопасности. Для управления безопасностью сети следует обратить внимание на требования, изложенные в стандартах серии ИСО/МЭК 18028.

Первым этапом защиты часто является заключение соглашения между организацией и провайдером телекоммуникационных услуг с учетом доверия к этим провайдерам. Поэтому использование известных провайдеров телекоммуникационных услуг с четкими соглашениями об уровне сервиса и соблюдение поло-

---

[1)] FIPS 140-2 развивается как международный стандарт ИСО/МЭК 19790 [35].

[2)] «Анализатор пакетов» является программой, анализирующей информационные пакеты во время их перемещения по сети и осуществляющей поиск информации, которая может использоваться для совершения атаки, например, на содержание сообщений электронной почты, имена и пароли пользователей или сетевые адреса.

жений контракта часто является первой и наиболее важной мерой защиты. Следующей наиболее важной мерой защиты сети является система мер защиты границ организации (см. 10.5), используемая для обеспечения безопасности, мониторинга и управления соединениями между внутренними и внешними сетями организации.

10.5 Меры защиты границ организации и ее связанности с внутренними и внешними сетями

10.5.1 Общие положения

Анализ источников [1]—[26] показывает увеличение открытости корпоративных сетей. То, что когда-то было прочной, жесткой контролируемой границей организации, стало открыто для веб-сервисов, делового сотрудничества, поддержки сторонними организациями, а также для взаимодействия клиентов с системами регистрации, временных работников с работниками по договору, и для доступа сотрудников — как удаленного из дома, так и их внешних соединений с другими фирмами. Все увеличивающаяся проницаемость границы организации означает, что она и системы взаимодействия продолжают являться критическими элементами информационной безопасности организации. Проницаемость границы организации также означает, что все больше устройств являются местами возможного проникновения для злоумышленников. Необходимо рассмотреть возможность применения для данных устройств межсетевых экранов, систем обнаружения вторжения и, возможно, других мер защиты (см. конечные системы в приложении D, раздел D.1).

Все границы между организацией и более крупной средой с сетевой структурой являются критичными; любая граница представляет возможность угрозам совершить атаку, используя уязвимости систем организации. Организации должны определить собственную политику, касающуюся путей применения мер защиты границы. Например, организация может потребовать изолирования корпоративной сети для создания безопасной среды с высокой степенью защиты, например, такой, при которой все пользователи и конечные системы будут физически связаны внутри здания организации. С другой стороны, организация может обеспечить защиту всех своих активов в безопасной базе данных за защитным сервером веб-приложений, при помощи многоуровневых межсетевых экранов и программных средств обнаружения вторжения или строгой аутентификации пользователей. Что из этих средств защиты является приемлемым, зависит от активов организации, оценки риска и принятых политик.

10.5.2 Межсетевые экраны

Межсетевые экраны представляют собой развитую технологию обеспечения защиты границы на сетевом уровне. В то время как существуют варианты реальных возможностей и способов функционирования, все межсетевые экраны располагаются между граничным маршрутизатором или коммутатором, соединяющими предприятие с другими объектами или Интернетом, и внутренними сетевыми маршрутизаторами организации. Хорошо спроектированный межсетевой экран является необходимым элементом обеспечения защиты сети организации.

Межсетевой экран осуществляет мониторинг сетевого трафика на основе адресации, портов, протоколов и, в некоторых случаях, содержания пакетов. Для многих организаций межсетевой экран открыт только для очень небольшого набора из всех доступных адресов, портов и протоколов. В качестве примера межсетевой экран, защищающий комплекс веб-сервера, может разрешать только протокол HTTP для порта 80 или протокол HTTPS для порта 443 (также известный как SSL). Другие обычные порты для FTP сервисов, SMTP (электронной почты) могут быть также открыты или закрыты в соответствии с потребностями и политиками организации.

Многие организации применяют два уровня межсетевых экранов для создания так называемой «демилитаризационной» зоны. Веб-серверы и другие направленные вовне серверы и сервисы размещают между уровнями межсетевых экранов и переформатируют и перенаправляют запросы трафика на услуги или данные внутри более крупного предприятия. Внешний межсетевой экран может поддерживать только http трафик, тогда как внутренний межсетевой экран может разрешать SSH или другие сервисы для поддержки доступа к управлению веб-серверами или разрешать доступ веб-серверов к внутренним базам данных. Обычной практикой является использование межсетевых экранов двух различных типов (производителей) на внутренних и внешних позициях.

Изначально межсетевые экраны считали программными средствами специального назначения или специальными устройствами, размещающимися на сетевом тракте и защищающими крупные участки организации. Межсетевые экраны были важным элементом прочности укрепленных периметров. В последние два-три года межсетевые экраны были включены в состав конечных систем, часто в качестве так называемых персональных межсетевых экранов. Обе тенденции — использование межсетевых экранов специального назначения для важных сетевых соединений и персональных межсетевых экранов на пер-

сональных компьютерах и других конечных системах — находятся в стадии развития. Новейшей тенденцией является комбинация функциональных возможностей межсетевых экранов с возможностью обнаружения вторжений.

10.5.3 Система обнаружения вторжений

Межсетевые экраны часто принимают или отвергают соединения на основе адреса, порта и протокола. В пределах этих параметров может существовать множество возможных потоков данных, фактически являющихся атаками или вредоносными программами (вирусами), а также множество легальных потоков данных, предназначенных для поддержки легального бизнеса. Системы обнаружения вторжений рассматривают данные в пакетах и сравнивают их с характеристиками известных атак. Затем системы обнаружения вторжений посылают предупреждения соответствующему персоналу организации при помощи электронного почтового сообщения, телефонного звонка или сообщения на пейджер. Существуют два основных вида систем обнаружения вторжения: первый — сетевые детекторы, подключенные к сетевым маршрутизаторам, коммутаторам и серверам и проверяющие трафик в сети; второй — детекторы на базе хоста, представляющие собой программное обеспечение, загруженное на серверы и конечные системы, проверяющие трафик, связанный с определенным устройством. Оба типа детекторов все шире используются в организациях[1)].

Одним из главных недостатков систем обнаружения вторжения является зависимость от атак с известными характеристиками, тогда как новые атаки с неизвестными характеристиками могут пройти незамеченными. Системы обнаружения вторжения начались с поиска отклонений в поведении систем, например, с появления ftp трафика там, где обычно присутствует только http трафик, или появления трафика в необычное время или в необычных объемах. Эти возможности обнаружения отклонений становятся все более изощренными и сложными, но их ценность по-прежнему в основном не доказана. Тем не менее, многие организации и большинство поставщиков систем обнаружения вторжения начали внедрять аналитические возможности систем обнаружения вторжения или проводить анализ поиска отклонений не только на внешних границах, но также в самой сети организации.

Некоторые аналитические средства зависят от других устройств для сбора данных, используемых для поиска отклонений. Существует тенденция к объединению систем обнаружения вторжений и межсетевых экранов; часто поставщик предлагает комбинированные средства, выполняющие функции межсетевого экрана и системы обнаружения вторжений. Данные комбинированные средства также используются в настоящее время — особенно если система обнаружения вторжений включает в себя свойства обнаружения отклонений для предотвращения вторжений. В этих новых системах предотвращения вторжений сетевое соединение, использованное для обнаруженной атаки, закрывается, чтобы остановить или предотвратить атаку до ее завершения. Хотя это является совершенно приемлемой практикой, существует возможность прохождения другого законного трафика через то же соединение. Каждая организация должна определить, перевешивает ли цена разрешения законного трафика убытки от возможного ущерба, нанесенного атакой.

Данная субъективная оценка в отношении допущения возможных атак в сопоставлении с вероятным ущербом от атаки выявляет один из недостатков систем обнаружения вторжений. Практически любая система обнаружения вторжений выдает некоторое число ошибочных результатов, то есть в некоторых случаях система обнаружения вторжений выдает предупреждение о трафике, выглядящим как атака, но в действительности являющимся легальным. Аналогичным образом существует (очень незначительная) вероятность того, что атака останется необнаруженной. Системы обнаружения вторжений обеспечивают организациям значительную гибкость в настройке систем с целью минимизации ошибочных результатов и ошибочных реагирований на атаки.

10.5.4 Другие защитные меры противодействия сетевым атакам

Существует много других защитных мер по противодействию сетевым атакам. Для разных способов атак требуются разные меры противодействия. Например, бизнес-партнер может иметь прямое соединение с внутренней сетью, маршрут может быть проложен через один (а не через два) межсетевой экран. Маршрутизаторы и коммутаторы, составляющие внутренние сети организации, должны быть надежно защищены и хорошо управляемы. Многие функции межсетевого экрана действуют как защитный уровень после функций маршрутизации, уже выполненных сетевой инфраструктурой. Вне сети межсетевых экранов и систем обнаружения вторжения существуют две другие основные меры противодействия: шифрование и аутенти-

---

[1)] Следует отметить, что в группе методов и средств обеспечения безопасности ИТ JTC 1/SC 27 начата работа по определению стандарта ИСО/МЭК 18043 [27].

фикация. Очевидно, что шифрование может использоваться для защиты частной информации. Его можно выполнить на многих уровнях и во многих местах, но за конкретную цену. Данные меры противодействия должны оцениваться с учетом политики и ценности информации организации.

Аутентификация может использоваться для идентификации устройств, а также пользователей устройств (включая пользователей программного обеспечения). Устройства можно идентифицировать, используя IPSEC, или (в некоторой степени) через протокол безопасности SSL. Конечный пользователь может быть аутентифицирован через SSL, хотя SSL не может реально аутентифицировать фактического пользователя — физическое лицо (некоторые браузеры, например, запоминают имена пользователей и пароли так, что сотрудник, использующий определенный компьютер и браузер для веб-сервера, будет казаться одинаковым). Использование различных факторов, а не только идентификатора пользователя и пароля, может улучшить качество аутентификации, но этого можно добиться также обладанием маркером или смарт-картой, секретным ключом, связанным с цифровым сертификатом, или отпечатками пальцев пользователя (или другими его биометрическими характеристиками).

11 Внедрение специальных средств защиты

11.1 Банковские карточки для финансовых операций

11.1.1 Общие положения

Банковские карточки для финансовых операций могут быть карточками с магнитной полосой, которые могут хранить информацию на магнитном носителе, или «смарт-картами»[1)], способными обрабатывать информацию, выполнять криптографические функции и хранить гораздо больше информации, чем на магнитном носителе. Поскольку смарт-карты обладают большей гибкостью, чем карточки с магнитной полосой, в будущем может быть разработан и другой метод использования этих карт. О безопасности смарт-карт см. стандарты серии ИСО 10202.

Ассоциации пользователей финансовых карточек поддерживают собственные стандарты минимальной безопасности для финансовых учреждений и подрядчиков, предоставляющих услуги финансовым учреждениям. В дополнение к этим программам обеспечения безопасности организации, использующие банковские карточки для финансовых операций, должны применять перечисленные ниже меры защиты.

11.1.2 Физическая безопасность

Для защиты от уничтожения, раскрытия или модификации информации на карточках для финансовых операций на стадиях обработки аппаратура персонализации карточек должна располагаться на территории, регулярно патрулируемой службами обеспечения правопорядка и обслуживаемой службами противопожарной защиты. Аппаратура должна быть защищена системой охранной сигнализации с автономным источником питания.

11.1.3 Злоупотребление со стороны инсайдеров

Для предупреждения мошеннических операций, осуществляемых в результате доступа к информации на банковских карточках, все носители, содержащие значимую информацию о счетах, номера счетов, личные идентификационные номера, кредитные лимиты и состояние счетов, должны храниться в помещении, доступ к которому ограничивается персоналом службы информационной безопасности. Функции изготовления и выпуска карточек должны быть физически отделены от функций изготовления и выпуска персональных идентификационных номеров.

11.1.4 Перемещение личных идентификационных номеров

Для предупреждения потерь из-за перехвата личных идентификационных номеров несанкционированными лицами с личными идентификационными номерами следует обращаться в соответствии с ИСО 9564-1-4 или ИСО 10202-1-8. Стандарты серии ИСО 9564 определяют основные принципы и методы обеспечения мер минимальной безопасности, необходимые для эффективного международного менеджмента личных идентификационных номеров. Они также определяют методы защиты личных идентификационных номеров, применяемые для операций с использованием банковских карточек для финансовых операций в условиях режима реального времени, и средства обмена данными личных идентификационных номеров. Стандарты серии ИСО 9564 также распространяются на менеджмент и безопасность личных идентификаци-

---

[1)] «Смарт-карта» определяет класс устройств размера платежной карточки, имеющих различные функциональные возможности и мощности. Эти устройства выглядят практически так же, как карточки с магнитной полосой, используемые для стандартных кредитовых, дебетовых, банкоматных и кассовых операций, и включают в себя карты на интегральных схемах (ICC), карточки с хранимой суммой и бесконтактные карточки.

онных номеров в условиях режима реального времени и условиях электронной торговли. Данные методы и средства должны использоваться организациями, отвечающими за внедрение методов менеджмента и защиты информации личных идентификационных номеров в банкоматах и финансируемых покупателями кассовых терминалах.

Примечание — ИСО 13491-1 [5] определяет средства управления распределения ключей, необходимые для устройств, предоставляющих финансовые услуги (кассовые терминалы, банкоматы).

Требования настоящего стандарта не распространяются на неприкосновенность данных об операциях, не имеющих личных идентификационных номеров, защиту личных идентификационных номеров от потерь или преднамеренного неправильного использования со стороны клиента или санкционированных служащих эмитента, защиту сообщений об операциях от изменений или замены, например реакцию санкционирования на верификацию личного идентификационного номера, защиту от воспроизведения личного идентификационного номера или операции, или определенные методы распределения ключей. Эти методы должны использоваться организациями, отвечающими за внедрение методов менеджмента и защиты персональных идентификационных номеров в банкоматах и финансируемых покупателями кассовых терминалах. Стандарты серии ИСО 10202 определяют принципы защиты интегральных микросхем в течение их жизненного цикла от производства и выпуска, использования клиентами и служащими до истечения срока службы. В стандартах серии ИСО 10202 также определяется минимальный уровень безопасности, требуемый для обмена, наряду с опциями безопасности, позволяющими эмитенту банковской карточки для финансовых операций или поставщику выбирать уровень безопасности, соответствующий политике приложений. Взаимосвязь с криптографическими ключами, надлежащее использование криптографических алгоритмов и методы распределения ключей, необходимые для обеспечения безопасности обработки финансовых операций, также определяются в стандартах серии ИСО 10202. В них также описываются требования безопасности для модулей приложений, которые могут быть добавлены к устройству считывания карточек.

11.1.5 Персонал

Для исключения обработки кредитных карточек персоналом, не имеющим права обработки, должны проводиться кредитные проверки и проверки уголовного прошлого всех служащих, имеющих дело с проштампованными или неиндоссированными карточками там, где это допускается нормативно-правовыми документами в области обеспечения безопасности, включая сотрудников, занятых неполный рабочий день, и временных работников.

11.1.6 Аудит

Для обеспечения целостности управляющей и регистрационной информации требуется мерами защиты и с использованием журнала аудита сохранять информацию о номерах счетов владельцев карточек и используемом оборудовании на пластиковых карточках с отпечатанными данными, в печатных формах, штамповочном и шифрующем оборудовании, на защитной фольге, голограммах, магнитной ленте, полуфабрикатах карточек и готовых карточках, карточках образцов.

11.1.7 Предупреждение подделки карточек

Для предупреждения создания фальшивых карточек с магнитной полосой использования информации, отражаемой на товарных чеках, должны быть зашифрованы цифры криптографической проверки, и эти цифры должны быть подтверждены как можно большему числу операций.

Для предупреждения создания фальшивых карточек с использованием перехваченной информации необходимо использовать физический метод идентификации карточки с целью подтверждения ее подлинности.

11.1.8 Банкоматы

Банкоматы представляют собой устройства, позволяющие клиенту проверять остаток на счете, изымать и вносить наличные, оплачивать счета или осуществлять другие функции, которые обычно ассоциируются с банковскими кассирами. Данные устройства могут находиться внутри зданий организации, размещаться за пределами такого здания или располагаться вдалеке от помещений организации.

Рекомендуются дополнительные меры предосторожности для снижения возможности ограбления клиентов и вандализма в отношении устройств, но они не рассматриваются в настоящем стандарте. Производители данных устройств и поставщики сети банкоматов обычно издают руководства по безопасности пользования банкоматами. Рекомендуется изучить эти документы. При работе с банкоматами необходимо соблюдать требования безопасности, которые определены в процедурах оплаты по карточкам.

11.1.9 Идентификация и аутентификация владельцев карточек

Наиболее распространенным средством аутентификации владельца карточки является PIN. Он используется для управления доступом к банкоматам и кассовым терминалам. Пользователи должны знать,

что обеспечение секретности персонального идентификационного номера является их обязанностью. В дополнение к персональному идентификационному номеру для идентификации владельцев карточек начинают применяться проверка биометрических данных и другие технологии.

Для предотвращения несанкционированных операций, вызванных угадыванием личного идентификационного номера карточки, используемых несанкционированным лицом, число попыток ввода личного идентификационного номера должно быть не более трех. После трех неудачных попыток рекомендуется задержание карточки и установление контакта с ее владельцем.

11.1.10 Аутентичность информации

Для предотвращения несанкционированного изменения информации, передаваемой в банкомат и из него, при каждой передаче следует требовать использования кода аутентификации сообщений, созданного в соответствии с требованиями ИСО 16609 и распространяемого в соответствии с требованиями стандартов серии ИСО 11568. Для предупреждения несанкционированного изменения, уничтожения или раскрытия информации, хранящейся в банкомате, физический контроль доступа к внутренней части банкомата должен соответствовать физическим средствам контроля защиты на денежных контейнерах.

11.1.11 Раскрытие информации

Для предотвращения несанкционированного использования банкоматов или кассовых терминалов посредством несанкционированного раскрытия информации о личном идентификационном номере, вводимого пользователем, должны использоваться только устройства с шифрующими клавиатурами, соответствующие требованиям стандартов серии ИСО 9564 [28]. Следует рассмотреть возможность шифрования всей информации, передаваемой из банкомата. Управление личными идентификационными номерами должно осуществляться в соответствии с требованиями международных стандартов.

11.1.12 Предупреждение мошеннического использования банкоматов

Для обнаружения и предотвращения мошеннического использования банкоматов, например подделки чеков, депозиты пустых конвертов или дезавуированные операции, рекомендуется целый ряд практических приемов. Данные приемы оправдываются в случае включения ограничения числа операций и суммы денежных средств, снимаемых в день с одного счета, ежедневного подведения баланса банкомата под двойным контролем, установки видеокамер, где вероятность совершения мошенничества велика, а также обеспечение поддержки работы банкомата в режиме «он-лайн», где это возможно, то есть требование, чтобы банкомат имел возможность проверки состояния счета до совершения операции. Если работа в данном режиме невозможна, следует установить более строгие требования к выпуску карточек, чем в случае работы в режиме «он-лайн».

11.1.13 Техническое обслуживание и текущий ремонт

Для предотвращения несанкционированного доступа к информации во время технического обслуживания и технического ремонта банкоматов следует убедиться, что для клиентов банкоматы находятся в состоянии «оф-лайн» перед проведением любого технического обслуживания. Для текущего ремонта банкоматов, включающего в себя открытые хранилища, необходимо установить процедуры двойного контроля.

11.2 Системы электронного перевода платежей

11.2.1 Несанкционированный источник

Угрозы и средства контроля, связанные с применениями электронного перевода платежей, могут оцениваться независимо от технологии, которую они используют. Для предотвращения потерь из-за принятия запроса о платежах от несанкционированного источника необходимо аутентифицировать источник сообщений, запрашивающих перевод платежей. Аутентификация источника должна быть основана на процедуре обеспечения безопасности, определенной в договоре с клиентом или корреспондентом. Применение этого средства контроля рекомендуется при условии целесообразности затрат на проведения криптографической аутентификации.

Криптографическая аутентификация обеспечивается кодом аутентичности сообщений, генерируемым в соответствии с требованиями стандартов серии ИСО 16609, с помощью криптографического ключа, распределенного в соответствии с требованиями ИСО 11568. В качестве альтернативы для установления подлинности источника сообщения может быть использовано успешное дешифрование сообщения, зашифрованного в соответствии со стандартами серии ИСО/МЭК 18033 (в соединении с ИСО ТО 19038 [29] или ANSI X.9.52 [30] или FIPS 197 [31]) ключом, распространяемым в соответствии со стандартами серии ИСО 11568. Также может использоваться цифровая подпись.

11.2.2 Несанкционированные изменения

Для предотвращения неправильного платежа из-за преднамеренного или случайного изменения содержания сообщения необходимо удостоверить дату платежа, дату зачисления денег, сумму, национальную

валюту, имя бенефициария и, возможно, номер счета бенефициария или IBAN-компоненты сообщения, используя процедуру обеспечения безопасности, определенную в договоре с клиентом или корреспондентом. Там, где это осуществимо, следует использовать полную аутентификацию текста. Рекомендуется применение криптографической аутентификации.

11.2.3 Воспроизведение сообщений

Для предотвращения несанкционированного повторного платежа, вызванного повторным введением сообщения, следует настоять на использовании и верификации уникальной идентификации сообщения. Рекомендуется включать эту идентификацию в любую проводимую аутентификацию.

11.2.4 Сохранение записей

В целях сохранения свидетельств, которые могут потребоваться для доказательства санкционирования при совершении платежа, регистрируйте сообщения с запросом о переводе платежей независимо от носителей, используемых для передачи сообщений. Следует сохранять материал, необходимый для подтверждения аутентификации, включая вспомогательный криптографический материал.

11.2.5 Правовая основа платежей

Для гарантии осуществления платежей в соответствии с подписанным договором, следует создать систему обеспечения наличия и корректности договоров, лежащих в основе запросов об электронном переводе платежей.

11.3 Банковские чеки

11.3.1 Общие положения

Банковские чеки, также известные как «платежные приказы» и «средства сберегательного счета клиента в банке», представляют собой письменные распоряжения, предписывающие финансовому учреждению выплатить деньги. Новые методы обработки чеков должны усилить озабоченность финансовых учреждений проблемами безопасности. Повышение престижа банковского чека и других средств сокращения процедуры работы с банковскими документами является примером методов, создающих проблемы с безопасностью. Национальными организациями многих стран были разработаны и опубликованы национальные стандарты по различным аспектам операций обработки чеков[1)].

11.3.2 Новые клиенты

Требование «знай своего клиента» создает особые проблемы, если услуги предоставляются через открытую сеть. Как бы ни были заманчивы услуги с применением базовой веб-страницы или другого электронного носителя, личное посещение офиса финансового учреждения остается необходимым условием для открытия нового счета (за исключением действия в соответствии с юридически установленным методом), пока не будет доступен повсеместно признанный и имеющий исковую силу электронный метод позитивной личной идентификации. Следует соблюдать обычные процедуры оценки квалификации клиентов.

11.3.3 Вопросы целостности

Каждая финансовая операция должна быть защищена с целью гарантирования идентификации, аутентичности пользователя, аутентичности сообщения, конфиденциальности информации ограниченного доступа и неотказуемости операций.

Запросы на финансовую операцию должны быть снабжены цифровой подписью с использованием ключа, санкционированного органом сертификации организации. При надлежащей реализации данной меры возможна гарантия, что пользователь идентифицирован, содержание сообщения не изменено и пользователь связан юридическими обязательствами в своих действиях.

Номера счетов, личные идентификационные номера или другие сведения, которые в случае их раскрытия сделают возможным несанкционированное использование счета, должны быть защищены с помощью шифрования.

12 Дополнительная информация

12.1 Страхование

Планируя программу обеспечения информационной безопасности, работник службы информационной безопасности и управляющий делами должны консультироваться со страховым отделом и, по возмож-

---

[1)] Подкомитетом В X9 (США) были опубликованы стандарты по операциям обработки чеков, например ANSI X9 TG-2. Понимание и разработка чеков и ANSI X9 TG-8 Принципы безопасности чеков. Для согласованного действия финансовых учреждений и улучшения качества обработки этим финансовым учреждения настоятельно рекомендуется следовать указаниям Технического руководства 2 (TG-2) X9 и Технического руководства 8 (TG-8) X9.

ности, со страховой компанией, что должно привести к созданию более эффективной программы обеспечения информационной безопасности и более эффективному использованию страховых премий.

Страховые компании могут потребовать, чтобы до того, как страховое требование было удовлетворено, были осуществлены определенные меры управления, называемые «условиями до наступления ответственности или предшествующими условиями». «Условия до наступления ответственности» часто связаны с мерами управления информационной безопасности. Поскольку эти меры управления используются для страховых целей, они должны быть включены в программу обеспечения информационной безопасности организации. Может также потребоваться гарантирование некоторых мер управления, т. е. демонстрация того, что они постоянно присутствовали с момента принятия политики.

Страховая компенсация прерываний бизнес-процесса и, в частности, ошибок и невыполнений, должна быть включена в планирование обеспечения информационной безопасности.

12.2 Аудит

Приведенная ниже цитата из «Заявления Института внутренних аудиторов» [32] определяет роль аудитора следующим образом: «Внутренний аудит является независимой и объективной деятельностью по консультированию и обеспечению доверия, предназначенной для придания значимости операциям организации и их совершенствованию, что содействует организации в достижении ее целей путем введения систематического и упорядоченного подхода к оцениванию и повышению эффективности процессов менеджмента риска, контроля и управления. При внутреннем аудите проверяется надежность и целостность информации, соответствие политикам и положениям, защита активов, экономное и эффективное использование ресурсов и действующие оперативные задачи и цели».

Говоря конкретнее, в сфере информационной безопасности аудиторы должны оценивать и тестировать защитные меры информационных активов финансового учреждения и постоянно взаимодействовать с работниками службы информационной безопасности и другими лицами для выработки соответствующих перспектив идентификации угроз и рисков, а также адекватности защитных мер для существующей и новой продукции.

Аудиторы должны предоставлять руководству объективные отчеты о состоянии среды управления, рекомендовать усовершенствования, которые могут быть оправданы необходимостью и анализом стоимости и эффективности, и предписывать порядок хранения и анализа информации журнала регистрации. В тех случаях, когда функция аудиторской проверки объединяется с другими функциями, для минимизации возможности конфликта интересов требуется особое внимание руководства.

12.3 Планирование восстановления деятельности организации после ее прерывания

Важной частью программы обеспечения информационной безопасности является план по продолжению критического бизнеса в случае его прерывания. Восстановление деятельности организации после ее прерывания является частью планирования возобновления бизнеса, которое гарантирует быстрейшее восстановление информации и средств обработки информации. В плане восстановления деятельность организации после ее прерывания определена совокупностью факторов воздействия, против которых необходимо обеспечить защиту, и функциями и обязанностями персонала в условиях прерывания.

План восстановления бизнеса после его прерывания должен включать в себя точный список действий, которые считаются наиболее важными, предпочтительно с категориями приоритета, а также периоды времени восстановления, являющиеся адекватными для выполнения бизнес-обязательств организации. В плане восстановления бизнеса должны быть определены запасные помещения для замены, обеспечивающие критически важную деятельность организации.

В случае неспособности персонала организации содействовать восстановлению деятельности организации после прерывания необходимо определить замещающий персонал, способный восстановить и эксплуатировать ресурсы обработки информации. По возможности, организация должна стараться заключить соглашения с поставщиками услуг об их приоритетном восстановлении. План восстановления деятельности организации после ее прерывания должен обеспечивать доступность адекватных дублирующих информационных систем, способных своевременно обнаруживать и извлекать критическую информацию.

Важно, чтобы в плане восстановления деятельности организации после его прерывания была определена информация, подлежащая резервированию, и было обеспечено безопасное хранение этой информации по установленной программе. Необходимо также определить местоположение хранения информации с учетом требований локального и удаленного расположения организации.

План восстановления после бедствия должен проверяться по мере необходимости для обнаружения проблем и продолжения обучения персонала в процессе его деятельности. Должна проводиться периодическая переоценка плана восстановления после прерывания бизнеса с целью проверки его актуальности. Организация должна определить минимальную периодичность проведения как проверок, так и переоценки восстановления после прерывания бизнеса.

12.4 Внешние поставщики услуг

Финансовые учреждения требуют, чтобы к предоставляемым извне критическим услугам, например, к обработке данных, финансовым операциям, сетевым услугам и созданию программного обеспечения, применялись защитные меры и защита информации такого же уровня, что и в самой организации. Контракты с внешними поставщиками услуг должны включать в себя элементы, необходимые для убеждения финансового учреждения в том, что:

- поставщики подчиняются практическим приемам и политике безопасности организации;
- отчеты, подготовленные консалтинговой бухгалтерской фирмой поставщиков, доступны организации;
- внутренние аудиторы организации имеют право проводить аудиты поставщиков, связанные с процедурами и защитными мерами организации;
- поставщики подчиняются условным соглашениям о поставленных системах, продукции или услугах.

В дополнение к вышеизложенному, специалисты конкретного финансового учреждения должны провести независимую финансовую проверку поставщика услуг до заключения с ним контракта.

До получения гарантийного письма, подтверждающего наличие защитных мер информационной безопасности, деловых отношений с поставщиком услуг быть не должно. Руководитель службы обеспечения информационной безопасности должен проверить программу обеспечения безопасности поставщика услуг для определения, согласуется ли она с программой организации. Любые разногласия должны разрешаться путем обсуждения условий с поставщиком услуг либо посредством процесса принятия риска в организации.

В дополнение к требованиям информационной безопасности договоры с поставщиками услуг должны включать в себя требования о неразглашении информации и четкое определение ответственности за убытки, являющиеся следствием недостатков в обеспечении информационной безопасности.

12.5 Группы тестирования на проникновение в компьютерные системы

Использование специалиста по тестированию на проникновение (как правило, подрядчика) для оценки эффективности безопасности системы посредством попытки проникновения в систему с ведома и при согласии соответствующего должностного лица организации является одной из предпосылок создания доверия к программе обеспечения безопасности.

По мере усложнения компьютерных систем поддержание безопасности становится все более затруднительным. Использование групп тестирования на проникновение может содействовать обнаружению слабых мест в системе организации. Однако необходимо учитывать некоторые дополнительные вопросы. Подрядчик должен быть связан соответствующими обязательствами или обладать достаточными возможностями для выполнения любых обязательств, возникающим в результате его действий.

Для контроля за своей программой обеспечения безопасности организация не должна полагаться только на отчеты тестирования на проникновение.

Проблема неразглашения результатов тестирования должна быть решена в контракте со специалистами по тестированию на проникновение. Любое разглашение проблемы безопасности должно осуществляться по усмотрению организации.

12.6 Криптографические операции

Развитие ИТ значительно усложнило традиционные методы контроля информации. Популяризация криптографических устройств предоставила финансовым учреждениям возможность вновь достичь ранее установленного уровня безопасности, связанного с банковским делом, с учетом усовершенствования технологии обработки информации.

Как в случае с любой новой технологией, существует опасность неправильного использования криптографических методов решения проблем обеспечения безопасности. Важно, чтобы организации принимали адекватные решения по выбору, использованию и постоянному оцениванию своих защитных мер, основанных на применении криптографии.

Предполагается, что потребность в криптографических защитных мерах общепризнана. В защитных мерах, предлагаемых в разделах 9—15, используются шифрование, коды аутентификации сообщений и цифровая подпись. Для каждой из этих мер также требуется разделение ключей и оказание услуг по их сертификации.

Криптографические защитные меры могут противодействовать угрозам нарушения конфиденциальности и целостности информации. Криптографические защитные меры, такие как шифрование и аутентификация, требуют сохранения секретности определенного материала, например криптографических ключей.

Для поддержки криптографических защитных мер могут потребоваться одно или несколько средств, генерирующих, распределяющих и несущих ответственность за криптографический материал. По возможности, должны использоваться международные стандарты по распределению ключей в банковском деле.

Средства, обеспечивающие управление криптографическим материалом, должны быть физически защищены на высшем уровне, и на таком же уровне должно быть управление доступом к ним. В целях безопасности информационной системы распределение ключей должно осуществляться по принципу разделенного знания.

При использовании надежных криптографических практических приемов и при эффективном планировании восстановления бизнеса после его прерывания могут возникнуть цели, противоречащие друг другу. Необходимы тесные консультации лиц, отвечающих за восстановление после бедствия, и лиц, ответственных за криптографическую поддержку, с тем, чтобы одна цель не противоречила другой.

Криптографический материал должен быть предоставлен клиентам так, чтобы минимизировать возможность компрометации. Клиент должен быть осведомлен о важности мер защиты криптографического материала. Взаимодействие с криптографической системой провайдера услуг, корреспондента или клиента должно допускаться только в соответствии с документированным гарантийным письмом.

Качество безопасности, создаваемой криптографической продукцией, зависит от постоянной целостности этой продукции. Как аппаратная, так и программная криптографическая продукция требует защиты целостности, сопоставимой с уровнем безопасности, который она предназначена обеспечивать. Использование сертифицированных интегральных схем, надежных корпусов и обнуления ключей упрощает защиту аппаратных систем в отличии от программных средств. При защите наиболее важной информации целесообразно использовать криптографическое программное обеспечение продукции. Для повышения целостности системы следует максимально использовать такие свойства, как самотестирование.

Использование, импорт и экспорт криптографической продукции регламентируются национальными нормативными правовыми актами государств. Национальные нормативные правовые акты в отношении использования, производства, продажи, экспорта и импорта криптографических устройств очень различаются. Рекомендуется консультация с юристом или местной властью.

12.7 Распределение криптографических ключей

Как и в любой технологии, существуют относительно простые, а также другие элементы, выполнение которых требует существенных усилий реализации и поддержки. Одной из таких технологий, применение которой требует тщательного планирования, обучения и точной реализации, является распределение криптографических ключей. Распределение криптографических ключей см. в стандартах серии ИСО 11568.

Распределение криптографических ключей представляет собой часть криптографии, которая обеспечивает методы безопасной генерации, обмена, использования, хранения и прерывания действия криптографических ключей, используемых криптографическим механизмом. Внедрение криптографических методов, таких как шифрование и аутентификация, в компьютерные системы и сеть может способствовать достижению многих целей безопасности. Однако эти методы бесполезны без надежного распределения криптографических ключей.

Основные функции распределения криптографических ключей состоят в предоставлении криптографических ключей, необходимых для криптографических методов, и защите данных ключей от любого вида компрометации. Конкретные процедуры и требования безопасности для распределения данных ключей зависят от вида системы криптографии, на которой основаны криптографические методы, их характера, характеристик и требований безопасности защищаемой компьютерной системы или сети.

Наиболее важным для изучения является вопрос о достаточной гибкости распределения криптографических ключей для эффективного использования в компьютерной системе или сети, и его соответствие требованиям безопасности системы. Услуги по распределению криптографических ключей должны быть доступны в любое время и там, где они потребуются, включая резервные помещения. Распределение данных ключей должно быть частью плана организации по восстановлению компьютерной системы или сети.

12.8 Неприкосновенность частной жизни

Финансовые учреждения обладают некоторой особо важной информацией об отдельных лицах и организациях. Национальные нормативные правовые акты требуют, чтобы эта информация обрабатывалась и хранилась в соответствии с определенными правилами обеспечения безопасности и неприкосновенности частной жизни. Некоторые технические и бизнес-разработки, например сети, графическое представление документов, целевой маркетинг и совместное использование информации между отделами, вызвали повышенный интерес к проблемам обеспечения неприкосновенности внутренней жизнедеятельности банков.

Организационно-распорядительные документы финансовых учреждений должны учитывать нормы обеспечения неприкосновенности частной жизни, например положения (руководства), связанные с информацией о кредитах. Следует также быть в курсе новых принимаемых национальных нормативных правовых актов о неприкосновенности частной жизни путем использования источников банковской индустрии или других независимых источников информации, а также консультации специалистов юридических отделов банков. Кроме того, банковские служащие, осуществляющие международные операции, должны обладать знаниями о региональных, международных и других законах и связанных с ними положениях обеспечения неприкосновенности частной жизни.

Финансовые учреждения должны анализировать свои операции с целью определения адекватности защиты информации о своих клиентах и служащих. Необходимо разработать конкретную политику и процедуры, касающиеся сбора, использования и защиты информации. Данная политика и процедуры должны быть доведены до сведения соответствующих служащих. Политика и процедуры обеспечения неприкосновенности частной жизни должны предусматривать:

- сбор достоверных и точных сведений, которые обеспечивают получение обозначенной финансовой потребности;
- обработку информации с целью обеспечения соответствующих ограничений доступа, включая определение круга лиц, которые должны иметь доступ к информации, контроль качества во избежание ошибок при вводе или обработке данных и защиту от непреднамеренного несанкционированного доступа;
- совместное использование информации посредством заранее определенных процедур с тем, чтобы информация использовалась для целей, имеющих отношение к причинам ее первоначального сбора, и коллективное использование информации не приводило к появлению новых возможностей несанкционированного вторжения в частную жизнь;
- хранение информации с гарантией ее защиты от несанкционированного доступа;
- уведомление об использовании информации и наличие процедур, позволяющих лицу, чья информация находится на хранении, исправлять в ней ошибки и запрещать использование этой информации;
- уничтожение ставшей ненужной информации.

Кроме того, электронные и другие формы контроля за действиями сотрудников должны соответствовать требованиям организационно-распорядительных документов, которые различаются по области ответственности и распространения. В дополнение к правам работодателей должны учитываться защита персональной информации служащих и их права.

Финансовые учреждения должны рассмотреть возможности проведения аудита неприкосновенности частной жизни. В ходе этого аудита проводится оценка, насколько хорошо организация выполняет защиту персональной информации, и рассматриваются способы, которыми ИТ может решать проблемы обеспечения неприкосновенности частной жизни.

13 Дополнительные защитные меры

13.1 Поддержка функционирования защитных мер

Поддержка функционирования защитных мер, включающая администрирование этих защитных мер, является важной частью программы обеспечения безопасности финансового учреждения. Обязанностью руководства на всех уровнях является обеспечение:

- четкого определения обязанностей по поддержке защитных мер;
- выделения ресурсов организации для поддержки защитных мер;
- периодической проверки и переоценки защитных мер с целью обеспечения продолжения их нормального функционирования;
- отсутствия воздействия изменений аппаратных/программных средств и обновлений системы ИТ на предполагаемую эффективность существующих защитных мер;
- отсутствия появления новых угроз или уязвимостей вследствие достижений в области технологий;
- обновления защитных мер и (или) добавления новых защитных мер при появлении новых требований;
- пересмотра и корректировки политики безопасности или добавление новой политики вследствие изменений защитных мер.

При условии выполнения описанных выше мероприятий поддержки можно избежать неблагоприятных и дорогостоящих последствий.

13.2 Соответствие требованиям безопасности

Проверка соответствия требованиям безопасности (аудит безопасности или анализ безопасности) является очень важным мероприятием и используется для обеспечения соответствия плану обеспечения безопасности информационных систем и поддержания эффективности соответствующего уровня информационной безопасности на протяжении срока службы системы или проекта ИТ. Оценку соответствия требованиям безопасности целесообразно проводить на стадиях проектирования, разработки и реализации информационных систем, а также при их совершенствовании и модернизации. Следует также соблюдать осторожность при замене или удалении компонентов системы.

Проверки соответствия требованиям безопасности могут проводиться с помощью внутреннего и внешнего персонала (например аудиторов). При проведении проверок соответствия требованиям безопасности частот используются перечни контрольных вопросов, связанных с политикой безопасности системы или проекта ИТ. Данные проверки должны планироваться и интегрироваться в разработки системы или проекта ИТ.

Дополнительным методом, особенно целесообразным при определении соблюдения требований персоналом, занимающимся операционной поддержкой, и пользователями определенных защитных мер и процедур, являются выборочные проверки. Выборочные проверки должны проводиться для гарантирования правильной реализации и использования надлежащих защитных мер безопасности, и, где это уместно, защитные меры должны проверяться тестированием. В случаях, если выясняется, что защитные меры не соответствуют плану обеспечения безопасности системы, необходимо уведомить об этом руководство проблемного сектора организации, создать, реализовать и протестировать план корректирующих мер, а результаты реализации этих мер — проанализировать.

13.3 Мониторинг

Мониторинг информационных систем представляет собой важный компонент плана обеспечения информационной безопасности. Мониторинг может служить для руководства показателем реализации защитных мер, то есть являются ли эти защитные меры удовлетворительными, и была ли реализована программа поддержки защитных мер. Первоначальный план обеспечения безопасности можно сравнивать с результатами мониторинга с целью определения эффективности защитных мер.

Многочисленные защитные меры вызывают необходимость создания журналов регистрации выходных данных, связанных с событиями безопасности. Эти журналы должны периодически просматриваться и, по возможности, анализироваться статистическими методами с целью раннего обнаружения изменений тенденций и повторяющихся неблагоприятных событий. Все изменения, связанные с активами, угрозами, уязвимостями и защитными мерами, потенциально могут оказывать существенное влияние на риски, а раннее обнаружение изменений позволяет принять предупредительные меры. Использование журналов регистрации только в целях анализа после событий означает игнорирование этого важного механизма защитных мер.

Мониторинг должен также включать в себя процедуры регулярного предоставления отчетов соответствующему работнику службы обеспечения информационной безопасности и руководству.

14 Разрешение инцидентов

14.1 Менеджмент событий

Событием в области безопасности является идентифицированное появление состояния в информационной или коммуникационной системе, которое указывает на возможное нарушение политики безопасности или на неспособность защитной меры обеспечить адекватную защиту актива. Любая ранее неизвестная или неожиданная ситуация может иметь отношение к безопасности и должна трактоваться как событие в области безопасности. Инцидентом безопасности является серия из одного или более нежелательных или неожиданных событий в области безопасности, которые обладают значительным потенциалом создания угрозы для информационной безопасности или причинения вреда бизнес-операциям. Появление событий в области безопасности неизбежно. Каждое такое событие должно расследоваться с целью определения, является ли оно инцидентом безопасности. Суть этого расследования должна быть соразмерна ущербу, причиненному событием, или потенциальному ущербу, который оно могло бы нанести.

Обработка инцидентов предоставляет возможность службе информационной безопасности реагировать на случайное или преднамеренное нарушение обычного функционирования системы ИТ. Необходимо разработать схему расследования инцидентов и представления отчетов о них, пригодную для всех систем ИТ и услуг организации. Данная схема должна включать в себя представление отчетов группам ИТ и бизнес-группам для получения более широкого представления о возникновении инцидентов информационной

безопасности и соответствующих угроз и связанного с ними воздействия на активы ИТ и бизнес-операции. Дополнительную информацию об урегулировании инцидентов и менеджменте событий см. в ИСО/МЭК 18044 [33].

Основными задачами во время расследования инцидента информационной безопасности является реагирование на инцидент наиболее подходящим и эффективным образом и извлечение уроков из инцидента информационной безопасности с тем, чтобы в будущем можно было избежать аналогичных неблагоприятных событий. В некоторых ситуациях может возникнуть (особенно для защиты репутации организации от критики неосведомленной недоброжелательно настроенной общественности) необходимость обеспечения защиты конфиденциальности информации, имеющей отношение к инциденту информационной безопасности.

Подготовленный план действий с заранее определенными решениями позволит организации осуществить реагирование в течение приемлемого срока с целью ограничения дальнейшего ущерба и там, где это возможно, продолжить бизнес-деятельность после применения дополнительных мер. План обработки инцидентов должен включать в себя требование хронологического документирования всех событий и действий. Данный фактор должен привести к определению источника инцидента. Он является предпосылкой для достижения цели, а именно снижения будущих рисков посредством улучшения защитных мер.

Важно также проведение и документирование анализа инцидентов с рассмотрением следующих вопросов:

- была ли надлежащим образом документирована хронология событий и действий;
- соблюдался ли план;
- была ли необходимая информация доступна соответствующему персоналу;
- была ли необходимая информация доступна своевременно;
- чем будут отличаться действия персонала в следующий раз;
- был ли эффективным процесс анализа инцидента (обнаружение/реагирование/представление отчета) или его можно усовершенствовать;
- существуют ли меры управления для предупреждения повторного возникновения связанного с безопасностью события?

Ответы на эти вопросы и принятие решений по полученным данным должны снизить вероятность появления инцидентов в будущем.

14.2 Расследования и правовая экспертиза

Для некоторых инцидентов требуется дополнительное расследование. Учащающиеся случаи мошенничества, недовольство служащих, а также некоторые правовые вопросы создают потребность в расследовании деятельности сотрудников в системах ИТ. Для поддержки расследования может потребоваться сбор и анализ системных журналов регистрации, журналов регистрации систем обнаружения вторжений и, иногда, всех накопителей на дисках. Могут потребоваться судебный анализ данных накопителя на дисках, включая поиск удаленных файлов, и другие виды детального анализа инцидента. Большинство организаций обладает только ограниченными внутренними возможностями для проведения таких расследований и анализа. Однако все программы обеспечения безопасности должны включать в себя минимальное обучение обработке свидетельств, плану проведения расследования и действиям лиц, проводящих расследование, а также выполнению разных видов правовой экспертизы. Реальные потребности расследования значительно различаются для различных организаций и различных инцидентов.

14.3 Обработка инцидентов

План обработки инцидентов должен быть хорошо известен всем, кто будет принимать участие в нем. В данном плане должны рассматриваться многие потенциальные проблемы:

- инциденты, происходящие во внерабочее время;
- потребности связи (как внутри организации, так и связь со средствами массовой информации и клиентами);
- планы резервирования и действий в чрезвычайных ситуациях;
- связь с поставщиками, включая бизнес-партнеров.

14.4 Проблемы, связанные с аварийностью

Для поддержания целостности информационных систем при аварийных ситуациях не следует пренебрегать процессами обеспечения безопасности. Необходимы специфические процессы, позволяющие осуществить исправление аварийных ситуаций в первую очередь для разрешения производственных проблем, и создания процедур скорейшего возврата к нормальной работе. При любых изменениях в информационных системах вносящие их лица, включая персонал поддержки в чрезвычайных ситуациях, должны документировать эти изменения и проводить необходимый анализ.

Приложение А
(справочное)

Образцы документов

А.1 Резолюция совета директоров по вопросу информационной безопасности

Постановили:

Информация является активом организации.

В качестве актива информационные ресурсы и ресурсы обработки информации организации должны быть защищены от несанкционированного или ненадлежащего использования.

Руководителю организации предписывается учредить программу обеспечения информационной безопасности, согласующуюся с приемлемой бизнес-практикой, с целью обеспечения надлежащей безопасности информационных активов организации.

А.2 Политика информационной безопасности

Политика информационной безопасности для финансового учреждения

Финансовое учреждение считает информацию в любой форме активом организации и нуждается в соответствующих защитных мерах для обеспечения защиты данного актива от несанкционированного или ненадлежащего использования. Информация необходима для эффективной и результативной повседневной работы организации. Информация должна использоваться только для выполнения заданной цели — ведения бизнес-операций финансового учреждения. Политика нашей организации состоит в предоставлении доступа к информации только на основе проверенного «принципа необходимого знания бизнеса» и отказе в доступе во всех других случаях.

Каждый старший менеджер подразделения финансового учреждения несет ответственность за поддержание конфиденциальности, целостности и доступности своих информационных активов и должен соблюдать все политики, стандарты и процедуры, опубликованные отделом информационной безопасности и касающиеся защиты информационных активов организации.

Все служащие обязаны осознавать, постоянно поддерживать и соблюдать политику, стандарты и процедуры организации, управляющие защитой информационных активов.

А.3 Договор с работниками в части их осведомленности

Организация считает информацию активом, который должен быть защищен.

Моя обязанность состоит в том, чтобы сознавать, поддерживать и соблюдать все политики, стандарты и процедуры организации, управляющие защитой информационных активов.

Мне был выдан экземпляр руководства по обеспечению информационной безопасности организации, и я согласен следовать приведенным в нем правилам.

Я согласен использовать информацию организации и оборудование для обработки информации, к которым я имею доступ, только для выполнения моих рабочих обязанностей.

Я понимаю, что организация может просматривать любую информацию или сообщения, которые я могу создавать, используя ресурсы обработки информации организации. Данные ресурсы включают в себя (но не ограничиваются ими) текстовые процессоры, электронные почтовые системы и персональные компьютеры.

Обязуюсь немедленно сообщать о любом подозрительном поведении или ситуации, которые могут создавать угрозу безопасности информационным активам организации, моему руководителю.

Я понимаю, что злоупотребление информационными активами организации может привести к дисциплинарному разбирательству, направленному против меня.

Дата _____

_____ _____

фамилия служащего подпись

_____

свидетель (или руководитель)

А.4 Экранные предупреждения при входе в систему

Данная частная компьютерная система является системой, доступ к которой ограничен несанкционированным лицам. Доступ санкционированных лиц ограничивается функциями, определенными для выполнения ими своих обязанностей. Любой несанкционированный доступ будет расследоваться и преследоваться в судебном порядке, если вы, не являясь полномочным пользователем, немедленно не отключитесь от системы.

В качестве альтернативы:

доступ к этой компьютерной системе разрешен только полномочным пользователям. Несанкционированный доступ/попытки доступа будут преследоваться в судебном порядке. Если вы не являетесь полномочным пользователем, отключитесь от системы.

А.5 Факсимильные предупреждения

Платежное предупреждение

ПРЕДУПРЕЖДЕНИЕ

Не полагайтесь на эту передачу при выплате денег или инициировании других операций без независимой проверки ее полномочий

Заявление о праве собственности

Документы, включенные в лист факсимильной передачи, содержат информацию корпорации, являющуюся конфиденциальной и/или предназначенной для ограниченного круга лиц, предназначенную для использования адресатом, чье имя указано на листке передачи. Если вы не являетесь адресатом, обратите, пожалуйста, внимание на то, что любое раскрытие, фотокопирование, распространение или использование содержания данного факсимильного сообщения запрещено. Если вы получили факсимильное сообщение по ошибке, пожалуйста, сразу же уведомите по телефону отправителя, для того чтобы мы могли организовать бесплатный возврат данных документов.

А.6 Информационный бюллетень по безопасности

Предупреждение о компьютерном вирусе

Согласно официальным сообщениям компьютерный вирус, известный как «вирус Микеланджело», быстро распространяется по всему миру и может оказаться наиболее разрушительным вирусом за последние годы. Известно, что он инфицирует системы на базе DOS с версией 2.xx или выше.

Воздействие

Данный вирус находится на инфицированных компьютерах и является бездейственным до даты его инициирования, то есть до 6 марта (день рождения Микеланджело). В этот день он перезаписывает критические данные системы, делая диск непригодным. Инфицированные данные включают в себя загрузочные данные и таблицу размещения файлов на загрузочном (гибком или жестком) диске.

Восстановление данных пользователя с поврежденного диска является крайне затруднительным.

Симптомы

Сообщаемые симптомы включают в себя:

- сокращение объема свободной/полной памяти на 2048 байт;
- непригодность гибких дисков или выведение странных символов при DIR командах.

Важно отметить, что вирус Микеланджело никогда не выводит никаких сообщений на экране ПК.

Риск инфицирования

Вирус распространяется в результате:

- загрузки с инфицированной дискеты (даже в случае безуспешной загрузки);
- загрузки с жесткого диска, в то время как инфицированная дискета находится в дисководе А и порт дисковода закрыт.

Носители данных, используемых в рабочих и домашних компьютерах, могут представлять риск с уровнем выше обычного.

А.7 Форма принятия риска

Принятие риска информационной безопасности

Данная форма должна заполняться, только если бизнес-процесс или система не соответствуют стандартам и политикам информационной безопасности и отсутствует план обеспечения соответствия данной политике в ближайшем будущем

Подразделение _____ Номер запрашивающего подразделения _____

Руководитель подразделения _____ Название запрашивающего подразделения _____

Страница и номер пункта в политике/стандартах _____ Дата _____

Принятие риска запрашивается для (привести описание)_____

_____

_____

_____

Описание бизнес-процесса (приложить дополнительную документацию при наличии) _____

_____

_____

_____

Общее число операций за период _____

Полный денежный объем операций за период _____

Является ли временной интервал операций зависимым? (привести описание)_____

Затронуты ли счета в общей бухгалтерской книге? _____

Уровень руководства, получающего выходные данные _____

Значимость решений, основанных на выходных данных _____

Нормативные/юридические действительные встречные удовлетворения _____

_____

Распространяются ли выходные данные среди клиентов? (привести описание) _____

Наивысшая степень секретности обрабатываемой информации _____

Привести описание системы, используемой для поддержки бизнес-процесса (приложить дополнительную документацию при наличии) _____

_____

_____

Описание типа оборудования (число компьютеров, типы и т. д.) _____

Описание типа связности узлов сети (локальная сеть, виртуальный телекоммуникационный метод доступа, коммутируемая телефонная связь и т. д.) _____

_____

Центры обработки _____

Число пользователей _____

Географическое распределение пользователей _____

Описать интерфейсы к другим системам _____

_____

Требования доступности _____

Работают ли на этом оборудовании другие приложения (привести описание) _____

_____

Поддерживаются ли системы группой центральных систем? Если нет, приведите описание имеющихся механизмов поддержки

_____

_____

Описание бизнес/системных требований соответствия политике _____

_____

_____

Приблизительная стоимость обеспечения соответствия _____

Описание используемых или предлагаемых защитных мер для уменьшения риска _____

_____

_____

Приблизительная стоимость используемых или предлагаемых защитных мер _____

Другие факторы, которые надо учитывать при принятии данного решения (другие рассмотренные альтернативы, дополнительные бизнес-факторы, действия других компаний и т. д.)

_____

_____

_____

Рекомендовано _____ Дата _____

руководитель подразделения

Проверено _____ Дата _____

ответственный за информационную безопасность

Комментарии: _____

_____

_____

Утверждено _____ Дата _____

руководитель с делегированными полномочиями

Номер документа принятия риска (присвоенный работником службы безопасности) _____

_____

Дата следующей проверки _____

Классификация информационной безопасности:

А.8 Договор с надомным работником и распределение работы

Договор о дистанционном присутствии между работодателем и работником

Настоящий договор имеет силу между _____ (в дальнейшем именуемым «Работником») и _____ (в дальнейшем именуемой «Компанией»). Стороны, намеревающиеся принять на себя юридические обязательства, договариваются по поводу следующего:

Объем обязательств по договору

Работник согласен оказывать услуги Компании в качестве надомного Работника. Работник согласен с тем, что дистанционное присутствие является добровольным и может быть прекращено Компанией в любое время по какой-либо причине или без нее.

Обязанности, обязательства и условия работы Работника Компании, отличные от обязанностей и обязательств, налагаемых на Работника, в прямой форме в соответствии с данным договором, остаются неизменными.

Термины «удаленное рабочее место» или «удаленное место работы» означают место жительства Работника или любое удаленное рабочее помещение, одобренное руководством Работника.

Условия договора

Данный договор вступает в силу со дня проставленной даты и остается в силе, пока Работник выполняет дистанционную работу, если не будет аннулирован раньше.

Аннулирование договора

Участие Работника в работе Компании в качестве надомника является полностью добровольным и предоставляется только тем Работникам, которые будут сочтены подходящими для этого по усмотрению Компании. Права дистанционного присутствия не существует. Однако, предлагая свои услуги и будучи выбранным для выполнения дистанционной работы, Работник принимает на себя обязательство выполнять дистанционную работу в течение нескольких месяцев. Компания не несет ответственности за расходы, ущерб или убытки, вытекающие из прекращения участия Работника в дистанционной работе. Данный документ не является договором о найме и не может толковаться как таковой.

Вознаграждение

Рабочие часы, сверхурочная работа, надбавки за работу в ночное время, отпуск: Работник согласен с тем, что рабочие часы, компенсация за сверхурочную работу, надбавки за работу в ночное время и график отпусков будут соответствовать условиям, согласованным между Работником и Компанией.

Оборудование для дистанционного присутствия и вспомогательное оборудование

Работник согласен с тем, что использование оборудования, программных средств, данных и мебели, предоставляемых Компанией для использования на дистанционном рабочем месте, ограничивается полномочными лицами в целях, связанных с бизнесом, включая самообразование, обучение и выполнение заданий. Работник использует телекоммуникационное оборудование строго в деловых целях. Компания не несет никакой ответственности за расходы на дистанционную связь, понесенные служащим при работе в личных целях.

Компания по собственному усмотрению может решить вопрос приобретения оборудования и соответствующих материалов для использования Работником при выполнении дистанционной работы или разрешить использование оборудования, находящегося в собственности Работника. Решение, касающееся типа, характера, функций и/или качества электронных аппаратных средств (включая компьютеры, факсы, видеотерминалы, принтеры, модемы, процессоры данных и другое терминальное оборудование, но не ограничиваясь ими), программного обеспечения, данных и телекоммуникационного оборудования (т.е. телефонных линий), остается исключительно в компетенции Компании.

Решение о перемещении или прекращении использования такого оборудования, данных и/или программных средств остается исключительно в компетенции Компании. Оборудование, приобретенное для использования Работником, остается собственностью Компании. Компания не несет ответственности за потери, ущерб или износ оборудования, находящегося в собственности Работника.

Работник определяет рабочее место в помещении для дистанционного присутствия с целью размещения и установки оборудования, которое будет использоваться во время работы. Работник должен поддерживать это рабочее место в сохранности и также обеспечить защиту от рисков сбоя и других опасностей для Работника и оборудования. Компания должна одобрить помещение, выбранное в качестве дистанционного рабочего места Работника. При внесении каких-либо изменений в первоначальное расположение аппаратуры на рабочем месте и настройке телекоммуникационного оборудования Компании расходы несет Работник.

Работник согласен с тем, что Компания может посещать дистанционное рабочее место с целью определения его безопасности и защищенности от рисков сбоя, а также для технического обслуживания, ремонта, инспектирования или изъятия являющегося собственностью Компании оборудования, программных средств, данных и/или ресурсов. В случае необходимости судебного процесса для возвращения оборудования, программных средств, данных и/или ресурсов в собственность Компании Работник согласен оплатить все расходы по ведению процесса, понесенные Компанией, включая оплату юриста, если Компания выиграет процесс.

В случае сбоев в работе или неисправности оборудования Работник согласен немедленно уведомить Компанию с целью осуществления немедленного ремонта или замены такого оборудования. В случае задержки с ремонтом или заменой или возникновения любых других обстоятельств, при которых Работник не сможет выполнять дистанционную работу, Работник должен быть готов к тому, что ему может быть поручено выполнять другую работу и/или он может быть переведен на другое рабочее место по усмотрению Компании.

Освещение, обстановка, оборудование для охраны окружающей среды и обеспечения безопасности бытовых приборов, являющиеся сопутствующими для используемого оборудования, программных средств и ресурсов Компании, должны применяться по назначению и поддерживаться в безопасном состоянии, и быть защищенным от дефектов и рисков сбоя.

Работник согласен с тем, что все данные, программные средства, оборудование, мощности и ресурсы, принадлежащие Компании, должны быть должным образом защищены. Данные, программные средства, оборудование и ресурсы, принадлежащие Компании, не должны использоваться для создания программных средств или личных данных Работника. Работник должен соблюдать все политики и распоряжения Компании, касающиеся конфликта интересов и обеспечения конфиденциальности. Любые программные средства, изделия или данные, созданные в результате связанной с основной работой деятельности, принадлежат Компании и должны производиться в утвержденном формате и на утвержденных носителях. Работник согласен с тем, что по окончании срока работы по найму он возвратит Компании все, что принадлежит ей.

Ответственность за ущерб

Работник осведомлен о том, что несет ответственность за вред, причиненный третьим лицам и/или членам семьи Работника в помещении Работника. Работник согласен ограждать и защищать Компанию, ее филиалы, сотрудников, подрядчиков и агентов от любых исков, правопритязаний и ответственности (включая связанные с этим потери, расходы, издержки и оплату юристов), возникших в связи с любым вредом (вплоть до летального исхода), причиненным людям или собственности (прямо или косвенно) услугами, предоставляемыми в силу данного договора Работником, в результате небрежности Работника, его халатных действий или недосмотра при выполнении обязанностей и обязательств Работника в соответствии с данным договором, за исключением случаев, когда эти иски, правопритязания и ответственность возникают исключительно из-за крайней небрежности или сознательного проявления халатности со стороны Компании.

Прочие условия

Работник согласен участвовать во всех исследованиях, опросах, отчетах и анализах, связанных с дистанционным присутствием, предназначенных для Компании, включая опросы, которые Работник может считать личными или конфиденциальными. Компания согласна с тем, что индивидуальные ответы Работника должны оставаться анонимными по просьбе Работника, но такие данные могут быть собраны и стать доступными общественности без идентификации личности Работника.

Работник осведомлен, что обязан соблюдать все правила, политики, практические приемы и указания Компании и условия данного договора и нарушение этого может привести к запрету на дистанционное присутствие и/или дисциплинарному взысканию, вплоть до увольнения.

Я подтверждаю, что ознакомился с данным договором и его содержанием. Я подтверждаю, что мне была предоставлена возможность ознакомить с данным договором моего адвоката перед его заключением.

Подпись Работника _____

Дата _____

Дистанционное присутствие или работа в каком-либо другом месте, например, на дому, является трудовой деятельностью, право на которую предоставляется некоторым Работникам при наличии взаимной выгоды для Компании и этих Работников.

Дистанционное присутствие — это не получение дохода работником, а альтернативный метод удовлетворения потребностей данной Компании. У Работника нет права на дистанционное присутствие. Компания может аннулировать данное соглашение в любое время.

Ниже приведены условия дистанционного присутствия, согласованные между надомным работником и его начальником.

Работник согласен выполнять следующие нормы и требования:

1) Работник будет осуществлять присутствие _____ дней в неделю.

2) Рабочие часы служащего будут следующими: _____

3) Ниже приводятся задания, над которыми будут работать служащие на дистанционном рабочем месте с предполагаемыми датами поставки: _____

_____

4) На дистанционном рабочем месте Работника будет использоваться следующее оборудование: _____

_____

5) Ниже приводится согласованный механизм оперирования телефонными звонками надомным работником с дистанционного рабочего места по делам Компании: _____

6) Рабочий согласен получать от _____ ресурсы, для работы в альтернативном месте; наличные выплаты за ресурсы, постоянно представленные в офисе Компании, обычно не возмещаются.

7) От Работника требуется регулярное посещение _____ центра для прохождения обучения и участия в совещаниях с рабочей группой и начальником.

Я ознакомился с представленным выше материалом с _____ до его участия в программе Компании по дистанционному присутствию

Дата _____ Подпись инспектора _____

Приведенный выше материал был обсужден со мной

Дата _____ Подпись Работника _____

Приложение В
(справочное)

Пример анализа безопасности веб-сервисов

В.1 Методические подходы к анализу безопасности

В.1.1 Обзор

Подобно политикам, которые могут быть высокоуровневыми или крайне детализированными, анализ риска может быть осуществлен с различными степенями детализации. В настоящем подпункте предоставлено обсуждение высоких уровней веб-сервисов, новой технологии, которая имеет значение для многих компаний, предоставляющих финансовые услуги, и других компаний, использующих Интернет для бизнеса. Данный пример анализа является иллюстративным и не должен рассматриваться в качестве конкретной рекомендации для обеспечения безопасности. Как отмечается на протяжении всего данного примера, каждая организация должна составить свое собственное определение риска и безопасности на основе своих конкретных политик и потребностей бизнеса.

Веб-сервисы являются общим термином для международных стандартов, сформированных на базе языка XML, которые позволяют компьютерам обмениваться данными и выполнять бизнес-функции и операции через Интернет. Основные функции веб-сервисов позволяют создавать информационные услуги доступа к другим компьютерам, чем визуально, через браузеры. Веб-сервисы являются достаточно мощными и способны обеспечивать взаимодействие внутри систем, подразделений и компаний.

Основными компонентами веб-сервисов являются:

- сервер приложений, где размещается сервис (т. е. где функционирует ПО сервера);
- интерфейс сервиса (часто описываемый на языке веб-сервисов, WSDL);
- хранилище данных или справочник с описанием интерфейса на WSDL, чтобы клиенты веб-сервисов могли найти (и использовать) интерфейс;
- клиент веб-сервиса, желающий использовать веб-сервис;
- протокол связи (простой протокол доступа к объектам, то есть SOAP), позволяющий клиенту веб-сервиса общаться с сервисом.

Существует большое число «определений» того, что составляет веб-сервис, но обычно общепринятым определением является информационная услуга, раскрывающая информацию через SOAP стандарта W3C [20]. Клиент интерфейса SOAP должен знать, как получить доступ к этим информационным услугам. Данный доступ может описываться в формате другого стандарта W3C, языка описания веб-сервисов (WSDL). Создатели сервисов на базе SOAP публикуют файлы WSDL.

В.1.2 Безопасность веб-сервисов

При обеспечении безопасности веб-сервисов необходимо рассматривать сервер приложений, поддерживающий сервис, описание сервиса, хранилище сервиса, клиента, использующего сервис, и протокол связи. Различными поставщиками была разработана структура безопасности веб-сервисов и ряд спецификаций. Кроме того, можно использовать универсальное решение проблемы веб-безопасности, SSL для обеспечения частичной безопасности веб-сервисов. В настоящем подпункте обсуждаются дополнительные подробности обеспечения безопасности веб-сервисов.

В.1.3 Стандарты безопасности

Файлы SOAP и WSDL представляют собой описание процедур обмена сообщениями и предоставления услуг соответственно, которые должны быть защищены для каждой из бизнес-услуг, в которой они используются. Однако в настоящее время они не являются совершенным средством обеспечения целостности данных, аутентификации источника или услуг обеспечения конфиденциальности для приложений веб-сервисов. Ожидается появление новых требований, а файл SOAP имеет структуру расширения, предусматривающую добавление элементов безопасности и протоколов в стандартизованном виде. Ниже приведен обзор некоторых стандартов безопасности, связанных с веб-сервисами.

Язык разметки систем гарантированной безопасности (SAML) определяет основанную на языке XML структуру обмена информацией по обеспечению безопасности, выраженной в виде утверждений в отношении логической единицы, имеющей тождество в некотором домене безопасности. Эти утверждения передаются в сообщениях запроса и ответных сообщениях на SAML. Обмен информацией по обеспечению безопасности происходит в форме утверждений на SAML, в которых могут передаваться подробности о предыдущих событиях аутентификации, атрибутах человеческих или компьютерных субъектов и решениях о санкционировании, разрешающих или запрещающих субъекту доступ к компьютерным ресурсам. Развитие SAML тщательно контролируется промышленностью, так как в перспективе он может стать стандартным средством передачи регистрационной информации для веб-сервисов, основанных на SOAP. В настоящее время у SAML существует описание SOAP.

Безопасность веб-сервисов представляет собой предлагаемую совокупность расширений SOAP, благодаря которой для операций веб-сервисов обеспечивается целостность и конфиденциальность. Целью безопасности

веб-сервисов является обеспечение целостности и конфиденциальности посредством распространения маркеров доступа, целостности и конфиденциальности сообщений. Предлагаемая компаниями Microsoft и IBM безопасность веб-сервисов и ответственность перешла к OASIS (организации по продвижению стандартов для структурированной информации).

Шифрование на языке XML является спецификацией W3C в формате передачи информации на языке XML методом стандартного шифрования. Шифрование на XML дает возможность шифровать и дешифровать цифровое содержание, включая в себя сам документ на языке XML на элементном, а не атрибутивном уровне. Спецификация также позволяет осуществлять безопасную передачу информации о ключе для дешифрования содержания документа на XML получателем.

Подпись на языке XML является проектом рекомендации объединенной группы IETF (проблемной группы проектирования Интернет) и W3C по представлению информации о цифровой подписи в документах на языке XML. Подписи на языке XML обеспечивают целостность, аутентификацию сообщения и/или услуги по аутентификации подписавшего лица для данных любого типа, расположенных в XML, включающем в себя подпись, или в другом месте. Подпись на языке XML является основным стандартом, на который дается ссылка в других стандартах безопасности, включая шифрование на языке XML, SAML и WS-Security.

Liberty Alliance Project является промышленным консорциумом, возглавляемым крупными фирмами, предназначенным для совместного открытого использования технологий интегрированной идентичности. Интегрированная идентичность позволяет потребителю использовать отдельную признанную идентичность во многих организациях. Этот потребитель может использовать ту же доверенную информацию об идентичности в группе различных организаций, и этому потребителю не надо представлять новую идентичность, мандаты идентификации собственности.

Распределение ключей на XML — это спецификация протокола W3C для описания и регистрации открытых ключей, которая может использоваться со спецификациями подписи и шифрования на XML. Распределение ключей на XML является версией спецификации 2. Инструментальные средства для распределения ключей имеются у различных поставщиков.

B.2 Стандарты веб-сервисов

B.2.1 Обзор

Стандарты для веб-сервисов постоянно совершенствуются. Тремя главными процедурами, дополняющими основные стандарты операций SOAP, являются: обнаружение сервисов, обеспечение безопасности и бизнес-процесс. Основным стандартом поиска сервисов служит UDDI (универсальная система предметного описания и интеграции), описывающая, как центральное хранилище файлов WSDL в открытом или частном исполнении позволяет пользователям находить и активизировать сервисы. Существует большое число используемых стандартов безопасности для обеспечения услуг по определению подлинности, шифрованию, подписанию и утверждению на уровне пользователя и сообщения. Стандарты бизнес-процесса связаны с ответом на вопрос: «Как я объединяю сервисы для создания целостного полезного процесса вместо элементарных функций?»

B.2.2 Внедрение

Для внедрения веб-сервисов требуется изучение риска или угроз, с которыми сталкиваются веб-сервисы, и мер безопасности по уменьшению этих угроз. Для такого анализа необходимо рассмотреть общую модель веб-сервисов, представленную на рисунке B.1 и относительно простой веб-сервис (WS1), который используется клиентами во всей сети организации. На рисунке B.1 показано, что четыре клиента могут запрашивать услуги веб-сервиса WS1. Необходимо отметить, что эти клиенты могут быть также веб-сервисами, таким образом, веб-сервис, предоставляющий клиенту функциональные возможности, может сам действовать как клиент, запрашивающий услуги у другого сервиса с целью осуществления собственных функциональных возможностей. Например, веб-сервис ипотечного калькулятора может зависеть от веб-сервиса определения ставок в вопросе предоставления услуги по расчету месячных платежей.

Возможно, что клиент S2 расположен на ближайшей сетевой шине, в том же информационном центре, что и WS1. Клиент S3 также находится во внутренней сети компании, но может быть гораздо дальше, например в филиале в другом городе или в другой стране. Клиент S4 находится в демилитаризованной зоне, соединенной с Интернетом, и имеет определенный уровень связи с Интернетом и внутренней сетью компании. Наконец, клиентам Интернета, таким как S5, возможен доступ к внутреннему сервису типа WS1.

B.2.3 Обеспечение безопасности

В отношении общих угроз требования безопасности для веб-сервиса WS1 обычно могут быть сведены к нескольким категориям. Во-первых, существует конфиденциальность входных данных в запросе услуги и конфиденциальность выходных данных, возвращающихся к клиенту. Целостность конфиденциальных данных также является предполагаемым или подразумеваемым требованием. Во-вторых, существует аутентификация и авторизация запроса клиента, удостоверяющие личность клиента и предотвращающие использование сервиса несанкционированными клиентами. Наконец, часто существуют некоторые регистрационные требования, позволяющие реконструировать операции и действия по трассировке. Для некоторых веб-сервисов могут существовать требования целостности данных без требований конфиденциальности.

Хотя требования безопасности для WS1 являются простыми, процесс принятия решения может быть довольно сложным. Например, процесс безопасной аутентификации между клиентом веб-сервиса и сервером веб-сервиса может осуществляться с помощью паролей, сертификатов и, возможно, другими методами. Хотя серти-

фикаты подтверждают требования безопасности, другие функциональные свойства сервера — эффективность, выравнивание нагрузки, обработка отказа — могут делать их внедрение проблематичным. В других сценариях может быть достаточно паролей, которые являются менее безопасными при определенных обстоятельствах. Например пароли, проходящие через память машины, могут обеспечивать достаточную безопасность для клиента, обращающегося к веб-сервису, работающему на той же аппаратуре. Если клиенты веб-сервиса располагаются дальше от сервиса, то могут потребоваться шифрованные пароли. Пароли могут шифроваться на прикладном уровне с помощью стандартов безопасности веб-сервисов, на транспортном уровне с помощью SSL или на сетевом уровне с использованием IPSEC (протокола безопасности IP). Требования обеспечения конфиденциальности входных и выходных данных могут аналогичным образом выполняться на прикладном, транспортном или сетевом уровнях.

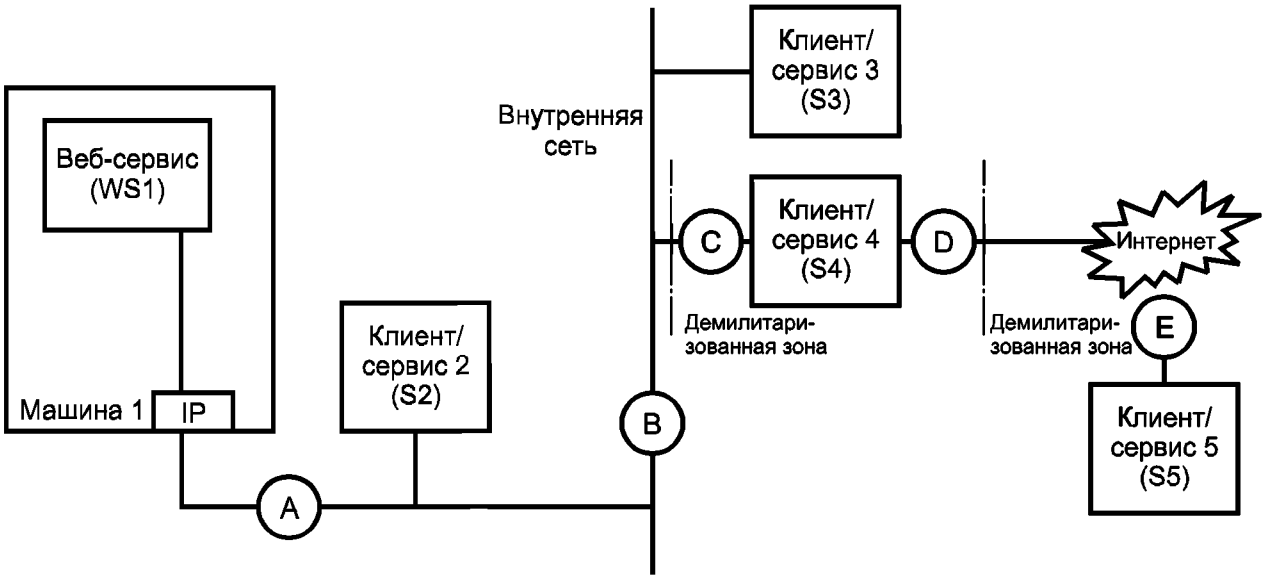


Рисунок В.1 — Общая модель веб-сервисов

Необходимо отметить, что требования аутентификации адресуются конкретно клиенту (который также является программным обеспечением), а не конечному пользователю. Веб-сервис может предполагать, что клиент аутентифицирует конечного пользователя, или веб-сервис может аутентифицировать конечного пользователя посредством информации в запросе веб-сервиса.

В.2.4 Анализ угроз

Угрозы WS1 включают в себя неправильное использование сервиса, отказ от обслуживания и несанкционированное использование сервиса. В большинстве случаев неправильное использование сервиса должно предотвращаться самим сервисом; WS1 должен проверять пригодность всех входных и выходных данных и выдавать сообщение об ошибке, если данные ввода-вывода выходят за ожидаемые предельные значения. Отказ от обслуживания можно устранить, создавая множественные варианты сервиса на различных машинах, используя запросы выравнивания нагрузки в вариантах сервиса и другие хорошо известные методы обеспечения доступности услуг ИТ. Несанкционированное использование предотвращается путем надежной аутентификации клиента, запрашивающего услугу. Конкретному веб-сервису может не требоваться аутентификация запросов клиентов или он может требовать очень строгой аутентификации запросов клиентов, в зависимости от характера веб-сервиса. Веб-сервис, перемещающий деньги между счетами, определенными в запросе, должен быть защищен; в противном случае он провоцирует лицо, организовывающее клиентов-мошенников, к запросу услуги перевода денег. Веб-сервис, рассчитывающий кредитные платежи на основе входных данных о кредите и процентных ставок по закладной, не нуждается в обеспечении безопасности, поскольку в действительности он является по существу калькулятором.

В.2.5 Решения

Решения по требованиям обеспечения безопасности веб-сервиса WS1 могут различаться в зависимости от клиентов, запрашивающих обслуживание. Рассмотрим случай, когда WS1 поддерживает только клиентов, подобных S2, которые расположены физически близко к WS1. В этом случае клиент и сервис расположены близко друг к другу, и возможность несанкционированных запросов на обслуживание может быть сведена к минимуму посредством таблиц маршрутизации, виртуальных локальных сетей, внутренних межсетевых экранов между сегментами сети или других методов. Предполагая, что WS1 и S2 достаточно защищены от внешних связей, логично

предположить, что конфиденциальность данных и аутентификация паролей основываются просто на их изоляции от остального мира.

По мере удаления клиента от веб-сервиса WS1 сложности возрастают. Между клиентом S3 и веб-сервисом WS1 запросы на обслуживание проходят по более широкой сети, открывая больше возможностей проверки запросов и больше точек, где может быть создан и введен несанкционированный запрос. Таким образом, между клиентом S3 и веб-сервисом WS1 требуется дополнительная защита. Как описывалось ранее, это может быть либо аутентификация на основе сертификатов, либо IPSEC между аппаратными средствами клиента S3 и аппаратными средствами веб-сервиса WS1.

Для клиента S4 нахождение в демилитаризованной зоне организации означает дополнительные проблемы безопасности. Демилитаризованные зоны используются для обеспечения прерываний, отделяющих Интернет от внутренних сетей. В силу обстоятельств системы в демилитаризованной зоне подвергаются большему риску и поэтому может потребоваться обеспечение дополнительной безопасности. Для клиента S4 комбинация безопасности прикладного уровня и транспортного или сетевого уровня может стать подходящим способом выполнения политик безопасности организации.

Наконец, что касается запросов веб-сервисов из-за пределов организации клиента S5, входящие запросы, вероятно, потребуют сложного решения. Идентификационная информация может быть защищена на прикладном уровне и безопасным образом передана через демилитаризованную зону, Интернет в веб-сервис WS1, так чтобы веб-сервис WS1 мог определить, уполномочен ли клиент S5 для запроса на обслуживание. Аналогичным образом, входные данные запроса могут быть зашифрованы на прикладном уровне, однако шифрование данных на прикладном уровне может быть завершено (или дешифровано) в демилитаризованной зоне, осуществлена проверка с тем, чтобы удостовериться, что данные находятся в пределах соответствующих параметров, затем вновь выполнено шифрование для передачи данных в веб-сервис WS1, где информация опять будет дешифрована. Таким образом, весь запрос веб-сервера может быть дополнительно зашифрован на транспортном или сетевом уровне для промежуточного сервиса (возможно клиента S4) в демилитаризованной зоне, который вновь создаст запрос веб-сервиса WS1 вероятно несколько в ином формате с тем, чтобы интерфейс веб-сервиса WS1 никогда не подвергался воздействию за пределами организации.

В кратком изложении обеспечения безопасности веб-сервисов делается вывод, что существует много возможных комбинаций механизма аутентификации, шифрования паролей и шифрования данных, которые отвечают различным потребностям аутентификации и конфиденциальности. Существует также множество мест в типовой сети организации, где могут использоваться веб-сервисы. Угрозы и необходимые контрмеры зависят от местоположения клиента веб-сервиса, сервера веб-сервиса, а также от сетевого тракта между двумя системами.

Существуют также другие концепции обеспечения безопасности веб-сервисов. Функционирование между клиентом и сервером часто бывает критически важным. Устранение отказа, резервирование, восстановление и вопросы, возникающие при непредвиденных обстоятельствах, могут сделать некоторые контрмеры более привлекательными. Инструментальные средства разработки веб-сервисов, имеющиеся в различных компаниях, обеспечивают различные виды поддержки стандартов SSL и стандартов безопасности веб-сервисов; конкретное инструментальное средство может не поддержать повторное использование SSL сеанса на основе сертификатов. Поскольку сервер приложений может обладать различными возможностями по отношению к стандартным инструментальным средствам, результаты могут различаться.

Приложение С
(справочное)

Иллюстрация оценки риска

Таблица С.1 — Форма оценки риска

Уязвимость	Риск финансовых убытков			Риск уменьшения продуктивности			Риск для репутации		
Персонал Идентифицировать уровень риска, вытекающего из следующей угрозы									
Несанкционированное раскрытие, изменение или разрушение информации	В	С	Н	В	С	Н	В	С	Н
Непреднамеренное изменение или разрушение информации	В	С	Н	В	С	Н	В	С	Н
Отсутствие подачи или неправильно адресованная подача информации	В	С	Н	В	С	Н	В	С	Н
Отказ от обслуживания или ухудшение обслуживания	В	С	Н	В	С	Н	В	С	Н
Помещения и оборудование Идентифицировать уровень риска, вытекающего из следующей угрозы									
Несанкционированное раскрытие, изменение или разрушение информации	В	С	Н	В	С	Н	В	С	Н
Непреднамеренное изменение или разрушение информации	В	С	Н	В	С	Н	В	С	Н
Отсутствие подачи или неправильно адресованная подача информации	В	С	Н	В	С	Н	В	С	Н
Отказ от обслуживания или ухудшение обслуживания	В	С	Н	В	С	Н	В	С	Н
Приложения Идентифицировать уровень риска, вытекающего из следующей угрозы									
Несанкционированное раскрытие, изменение или разрушение информации	В	С	Н	В	С	Н	В	С	Н
Непреднамеренное изменение или разрушение информации	В	С	Н	В	С	Н	В	С	Н
Отсутствие подачи или неправильно адресованная подача информации	В	С	Н	В	С	Н	В	С	Н
Отказ от обслуживания или ухудшение обслуживания	В	С	Н	В	С	Н	В	С	Н
Системы связи Идентифицировать уровень риска, вытекающего из следующей угрозы									
Несанкционированное раскрытие, изменение или разрушение информации	В	С	Н	В	С	Н	В	С	Н
Непреднамеренное изменение или разрушение информации	В	С	Н	В	С	Н	В	С	Н
Отсутствие подачи или неправильно адресованная подача информации	В	С	Н	В	С	Н	В	С	Н
Отказ от обслуживания или ухудшение обслуживания	В	С	Н	В	С	Н	В	С	Н

Окончание таблицы С.1

Уязвимость	Риск финансовых убытков			Риск уменьшения продуктивности			Риск для репутации		
Программные средства среды и операционные системы Идентифицировать уровень риска, вытекающего из следующей угрозы									
Несанкционированное раскрытие, изменение или разрушение информации	В	С	Н	В	С	Н	В	С	Н
Непреднамеренное изменение или разрушение информации	В	С	Н	В	С	Н	В	С	Н
Отсутствие подачи или неправильно адресованная подача информации	В	С	Н	В	С	Н	В	С	Н
Отказ от обслуживания или ухудшение обслуживания	В	С	Н	В	С	Н	В	С	Н

С.2 Описание табличной формы оценки риска

С.2.1 Зоны уязвимости

Табличная форма оценки риска представляет собой одностраничную форму, предназначенную для использования в оценке риска бизнес-функций. Табличная форма включает в себя пять зон уязвимости:

1) персонал;
2) помещения и оборудование;
3) приложения;
4) системы связи;
5) программные средства и операционные системы.

С.2.2 Потенциальные угрозы

Под названием каждой зоны уязвимости в таблице С.1 перечислены четыре подлежащие оценке потенциальные угрозы:

1) несанкционированное раскрытие, изменение или разрушение информации;
2) непреднамеренное изменение или разрушение информации;
3) отсутствие подачи или неправильно адресованная подача информации;
4) отказ от обслуживания или ухудшение обслуживания.

С.2.3 Уровни и категории риска

Справа от каждой угрозы приведены степени риска в трех категориях — финансовые убытки, уменьшение продуктивности, ущерб для репутации. Политика, программа и процедуры информационной безопасности представляют собой средства менеджмента риска, которые используются организацией для оценки и уменьшения бизнес-риска. Риск финансовых убытков в доходах или капитале организации может возникать из-за проблем с услугами, информационными системами или поставкой продукции. Степень этого риска определяется честностью служащих, состоянием внутренних средств защиты, информационных систем и рабочих процессов.

Риск, относящийся к доходам, капиталу и бизнес-репутации, вытекающий из негативного общественного мнения, может воздействовать на способность финансовых учреждений устанавливать новые взаимосвязи или услуги или поддерживать существующие. Риск может привести организацию к судебному процессу, финансовым убыткам или дальнейшему ущербу для репутации. Продолжительный риск для доходов или капитала, вытекающий из нарушения законов, правил, положений, предписанных практических приемов, этических норм или из-за несоответствия им может подвергнуть финансовое учреждение штрафам, гражданско-правовым денежным санкциям, необходимости возмещения ущерба и потере контрактов.

В данном стандарте используются следующие степени риска:

- высокая (В) — значительные финансовые убытки, уменьшение продуктивности или ущерб для репутации, вытекающие из угрозы, появляющейся вследствие соответственной уязвимости;
- средняя (С) — незначительные финансовые убытки, уменьшение продуктивности или ущерб для репутации;
- низкая (Н) — минимальная возможность финансовых убытков, уменьшение продуктивности или ущерб для репутации или полное отсутствие этих потерь.

С.2.4 Инструкции по оценке риска

Табличная форма заполняется путем определения степени риска — высокого (В), среднего (С) или низкого (Н) — по воздействию каждой категории угроз на каждую из пяти категорий уязвимостей, имеющих отношение к бизнес-функции. Для оценки рисков организации необходимо:

- проанализировать значение каждой из потенциальных угроз в табличной форме для оцениваемой деловой функции;

- определить, как и кто будет подвергаться риску и какова степень риска, вытекающего из каждой потенциальной угрозы, являющейся следствием конкретной категории уязвимости.

При определении степени риска не существует абсолютных правил. Определение колебаний валютных средств, изменение трудоемкости работ и наихудших вероятных событий может принести значительную пользу. При возникновении сомнений во время анализа потенциальных угроз следует учитывать возникновение наихудшего события и выбирать для него более высокий уровень риска.

При заполнении табличной формы оценки риска основное предположение должно заключаться в том, что никаких защитных мер не существует.

В качестве примера первую угрозу в таблице С.2 можно проанализировать следующим образом:

- может ли привести к денежным потерям, уменьшению продуктивности или ущербу для репутации учреждения, если лицо, имеющее обычный доступ, раскрыло информацию о вашей аппаратуре и оборудовании (то есть служащий отдела раскрыл комбинацию сейфа отдела, содержащего ценности или конфиденциальную информацию);

- будет ли уровень убытков и/или ущерба для репутации высоким, средним или низким.

Идентифицированные угрозы (т. е. служащий отдела раскрыл комбинацию сейфа отдела, содержащего ценности или конфиденциальную информацию) должны быть документированы вместе с использованным логическим обоснованием. Некоторым бизнес-функциям может соответствовать ответ «неприменимо» в отношении какой-либо угрозы, возникшей вследствие некой уязвимости или целой категории уязвимостей. В этом случае необходимо документировать логическое обоснование, лежащее в основе решения, а документацию — сохранить в файле с заполненной табличной формой.

После идентификации угроз возникает необходимость принятия рисков при наличии соответствующих полномочий либо смягчения рисков. Риски могут быть смягчены передачей риска (страхование), принятием мер противодействия в отношении рисков (снижение) путем применения средств управления безопасностью или избежания риска посредством устранения источника угроз через изменение бизнес-цели.

С.3 Таблица оценки риска

Для каждой категории риска необходимо ввести степень риска, связанную с каждой уязвимостью: высокая (В), средняя (С) или низкая (Н). При оценке каждой категории риска определяется общий риск для конкретной уязвимости. После заполнения таблицы С.2 выбирают подходящие средства управления.

Таблица С.2 — Оценка риска по категориям уязвимости

Уязвимости	Категория риска			
	Финансовые убытки	Уменьшение продуктивности	Ущерб для репутации	Общий риск
Персонал				
Аппаратура и оборудование				
Приложения				
Системы связи				
Программные средства среды и операционные системы				

С.4 Описание таблицы оценки риска

С.4.1 Краткий обзор

Таблица С.3 — таблица оценки риска используется для показа общей степени риска для каждой уязвимости. В верхней части таблицы перечислены три категории риска, а пять зон уязвимости — в левой колонке таблицы.

Таблицу оценки риска заполняют путем установления общей степени риска для каждой из пяти зон уязвимостей. Общая степень риска должна быть выведена из четырех угроз, ранее идентифицированных в таблице С.1.

С.4.2 Инструкция по таблице рисков

В целях объединения риска для конкретной категории следует изучить степени риска для каждой уязвимости в таблице С.3. В каждой категории риска в отдельности следует определить вид общей степени риска для четырех угроз. В таблицу оценки риска записывают степень риска.

Для установления общего риска после проведения оценки каждой категории риска следует проанализировать логическое обоснование, стоящее за степенью риска, установленной для каждой уязвимости, и оценить общий риск — высокой (В), средней (С) или низкой степени (Н) — для каждой уязвимости.

Следует учесть, что при определении общих степеней риска для каждой уязвимости не существует общих правил. Однако следует учитывать следующие факторы:

- возможность или вероятность возникновения угрозы. Угрозы с большей вероятностью возникновения должны оказывать более существенное влияние на определение степени риска, угрозы с наименьшей вероятностью возникновения — менее существенное влияние;

- угрозам, имеющим прямое отношение к оцениваемой бизнес-функции, при определении степени риска необходимо придавать большее значение.

Следует проявлять осторожность при оценке степени риска и в случае сомнения выбирать более высокую степень риска.

В качестве примера оценки общего риска угрозе отсутствия или неправильно адресованной подачи информации может служить большая значимость при выборе степени общего риска, так-как отсутствие поставки может считаться более значимой угрозой для анализируемой бизнес-функции, чем несанкционированное раскрытие информации о поставке.

С.4.3 Выбор средств управления

Выбор защитных мер безопасности обеспечивает учреждению непосредственное управление принимаемым риском. Учреждение должно оценить, насколько запланированные и существующие защитные меры снижают риск, идентифицированный при анализе риска, определить дополнительные имеющиеся защитные меры или меры, которые могут быть скомпрометированы, разработать архитектуру безопасности ИТ и определить ограничения различных типов (см. 8.3—8.7). Затем необходимо выбрать соответствующие обоснованные защитные меры для снижения оцененных рисков до приемлемого уровня. Дополнительные подробности о выборе защитных мер см. [2], [5], [20], [21].

С.4.4 Ранжирование воздействия и вероятности

Для определения степени вероятности воздействия используют шкалу ранжирования от 1 до 9. Оценка масштаба вероятности и определенного воздействия по каждой из шести основных категорий структуры рисков организации устанавливается исходя из практической деятельности организаций. Данная градация дает ощущение «дискретности», однако значения должны рассматриваться как рекомендации по определению величины риска, а не в качестве руководства к применению.

Для определения вероятности принята следующая шкала ранжирования:

- пренебрежимо малая — один раз в 1000 лет или реже;
- крайне маловероятная — один раз в 200 лет;
- очень маловероятная — один раз в 50 лет;
- маловероятная — один раз в 20 лет;
- возможная — один раз в 5 лет;
- вероятная — ежегодно;
- очень вероятная — ежеквартально;
- ожидаемая — ежемесячно.
- ожидаемая с уверенностью — еженедельно.

Предполагается, что вероятность наступления рискового события выбранного ранга в четыре раза превышает предыдущую вероятность.

В таблице С.3 приведены общие параметры оценки риска и характеристики каждого из шести основных категорий риска. Для некоторых оценок риска могут потребоваться другие характеристики, но используемые степени вероятности наступления рискового события должны соответствовать шкале ранжирования.

Следует отметить, что оценка приводится для чистого, а не для общего риска. Другими словами, необходимо уделять внимание рисков при наличии имеющихся мер управления. Обычно наличие предупреждающих мер управления снижает вероятность возникновения события, но не влияет на степень его воздействия; меры управления, специально направленные на уменьшение воздействия, обычно не влияют на степень вероятности возникновения события.

Таблица С.3 — Оценка риска

Ранг		Описание	Репутация	Операционный риск	Безопасность	Правовой риск	Финансовый риск	Стратегический риск
НИЗКИЙ	1	Пренебрежимо малое			Локальный пароль к не секретным данным раскрыт, но не использован		<$ 100	

Продолжение таблицы С.3

Ранг		Описание	Репутация	Операционный риск	Безопасность	Правовой риск	Финансовый риск	Стратегический риск
НИЗКИЙ	2	Очень незначительное	Нападки на банковскую систему по местному радио и в местной прессе	Незначительное количество эксплуатационных проблем, не оказывающих воздействие на клиентов	Локальный пароль к секретным данным раскрыт, но не использован	Правовые ответы от участника клиринга не выполняются во временной период, определенный законом	~$ 1000	
	3	Незначительное	«Стандартные» язвительные высказывания в национальной прессе или размещенные в Интернете о банковской системе, например письмо читателя	Временное невыполнение обслуживания (~1 ч) одного члена системы; проблемы, оказывающие ограниченное влияние на клиентов	Утечка или компрометация незначительного количества текущей информации	Идентифицирована поправимая возможность несоответствия	~$ 5000	Политики или стандарты не поддерживаются
СРЕДНИЙ	4	Заметное	Внимание национальной прессы или радио, например плохой отзыв	Эксплуатационные проблемы, оказывающие воздействие на всю систему клиринга	Злоупотребление законными привилегиями доступа	Неспособность предоставить данные, требуемые законом, например, согласно [11]	~$ 20000	
	5	Существенное	Серьезная критическая статья в прессе или документальная передача по радио или по телевидению, склонная рассматриваться как исходящая из заслуживающего доверия источника	Временное невыполнение обслуживания многих членов системы или длительное невыполнение обслуживания (до одного рабочего дня) для одного члена системы; существенное воздействие на клиентов	Логическое или физическое проникновение в операционные системы одного или более членов системы (например вредоносный вирус, причинивший некоторый ущерб)	Правовое вмешательство, иск не удовлетворен	~$ 100000	Политики или стандарты не существуют

Окончание таблицы С.3

Ранг		Описание	Репутация	Операционный риск	Безопасность	Правовой риск	Финансовый риск	Стратегический риск
СРЕДНИЙ	6	Очень существенное	Публичная критика со стороны национального регулирующего органа или отраслевого	Член системы не может работать с клирингом	Успешное мошенничество мелкого — среднего масштаба	Начало полицейского или регулятивного расследования; регулятивное вмешательство; иск удовлетворен	~$ 1000000	
ВЫСОКИЙ	7	Большое	Ведущая новость во многих газетах и/или основных телевизионных новостях	Невыполнение обслуживания для многих членов системы в критическое время дня (15:00, пятница)	Успешное мошенничество крупного размера; операционные данные или системы контроля скомпрометированы	Судебное преследование, возбужденное против клиринговой палаты (неуспешное)	~$ 10000000	Управленческий контроль скомпрометирован
	8	Очень большое	Государственное вмешательство или сопоставимые политические последствия	Невыполнение клиринга в течение всего рабочего дня	Клиринговая система взлома и серьезно скомпрометирована	Судебное преследование, возбужденное против клиринговой палаты (успешное)	~$ 100000000	
	9	Катастрофическое	Широкое освещение прессой и телевидением, полная потеря доверия со стороны публики и членов системы	Полное невыполнение обслуживания в течение нескольких дней/недель	Клиринговая палата или ее криптографические системы полностью скомпрометированы; мошенничество крупного масштаба без известной оценки	Систематическое и умышленное несоблюдение закона руководством высшего уровня	~$ 1000000000	Будущее существование клиринговой палаты под сомнением; платежная индустрия скомпрометирована

Подверженность риску или значимость риска

Формируется модель, используемая как средство определения подверженности риску на основе ранжирования по воздействию и вероятности. Данная модель включает в себя пять уровней. На практике категории риска, оцениваемые уровнем 1, не заслуживают дальнейшего анализа. Оцениваемые уровнем 5 подлежат немедленному реагированию, а не продолжению оценки риска! Так что в целом мы получаем трехуровневую шкалу.

Обозначение заливки:
незащищенность от воздействия/значительность:

критическая	5
значительная	4
существенная	3
незначительная	2
пренебрежимо малая	1

влияние	9	3	3	4	4	4	5	5	5	5
	8	3	3	4	4	4	4	5	5	5
	7	2	3	3	3	4	4	4	5	5
	6	2	2	3	3	3	4	4	4	5
	5	2	2	2	3	3	3	4	4	4
	4	1	2	2	2	3	3	3	4	4
	3	1	1	2	2	2	3	3	3	4
	2	1	1	1	2	2	2	3	3	3
	1	1	1	1	1	2	2	2	3	3
		1	2	3	4	5	6	7	8	9
		Вероятность								

Несомненно, что чем больше значимость риска, тем больше усилий нужно затратить на анализ и управление риском. На этой стадии не стоит слепо следовать системе оценки; самым необходимым является определение основных проблем риска, которые будут рассматриваться руководством в любом уместном для него порядке на основе всей имеющейся информации, включая подверженность риску, но не ограничиваясь ей. К факторам, которые следует принимать в расчет на этой стадии, относятся обычные факторы, регулирующие управление бизнесом: наличие ресурсов, бюджет, стратегия и цели компании в данное время, политическое влияние и т. д.

Последующие действия

Для обработки идентифицированных рисков выбирается одно из следующих четырех направлений действий:

- избежание — означает устранение источника угрозы или изменение бизнес-цели для устранения риска. Хотя этот способ обработки риска кажется идеальным, он, очевидно, применим лишь в редких случаях. «Без риска нет бизнеса!» Например, вы можете избежать риска быть сбитым машиной, никогда не выходя из дома, но в этом случае значительная часть жизни пройдет мимо вас. Приведем пример, более близкий к бизнес-операциям: мы можем предотвратить воздействие несостоятельности третьей стороны, не используя эту сторону, в этом случае нам, вероятно, просто не с кем будет работать! Однако в тех случаях, когда риска можно реально избежать, это часто является дешевым и долгосрочным решением;

- принятие мер — означает, что необходимо осуществить действия, которые заключаются в разработке плана. Выполнение этих действий уменьшает вероятность материализации риска или ограничивает эффект события и таким образом уменьшает его воздействие. Примеры многочисленны и очевидны — принятие мер в отношении риска потери данных с помощью режима резервного копирования, ограничение эффекта компрометации криптографических ключей путем ограничения срока их службы и т.д.;

- распределение — означает переложение основной части воздействия последствий риска на третью сторону. Классическим способом является страхование. Несомненно, распределение риска редко достигается без определенных текущих расходов! Например, мы можем распределить нашу ответственность за выдачу некачественной консультации путем профессиональной компенсационной политики. Риски иногда можно распределить на третьи стороны через соглашение (как ответственность), хотя способность этих сторон управлять последствиями рисков сама по себе может представлять риск;

- принятие — четвертым вариантом является простое принятие риска. Необходимо осознать возможность появления риска, но оценив расходы и степень желательности трех первых вариантов, принять решение о том, что величина риска перевешивается потенциальными выгодами работы с ним. Например, мы можем решить

принять риск физического доступа в помещения преступников с огнестрельным оружием потому, что стоимость физических мер безопасности очень высока и их установка неблагоприятно повлияет на атмосферу благожелательности в нашей компании.

Конечно, можно использовать смешанные подходы к определению рисков, например, в случае проникновения вооруженных преступников в помещение принимается высокая степень риска, а в отношении меньших угроз (например люди, случайно зашедшие с улицы), принимается более низкая степень риска, применяется мера — используется невооруженная охрана помещений. В качестве меры ликвидации последствий от этой угрозы используется обеспечение дополнительного доступа сотрудников с клавишным вводом личного идентификационного номера к ключевым зонам или сужением функции путем передачи части риска через оформление страхования жизни сотрудников.

Остаточные риски

Необходимо определить действия по мониторингу для осуществления менеджмента остаточных рисков, а также ответственность за эти действия.

Приложение D
(справочное)

Технологические средства управления

D.1 Аппаратные средства

D.1.1 Средства управления конечной системой

Большинство организаций сегодня использует определенные комбинации настольных и переносных ПК в качестве основных ориентированных на пользователей систем. В этих конечных системах используются различные операционные системы, хотя их преобладающее большинство предоставляется одним поставщиком. Кроме того, данные ПК дополняются или в некоторых случаях заменяются небольшими персональными информационными устройствами (ПИУ). Сотовые телефоны также становятся более мощными и могут иногда использоваться как конечные системы. Специалисты в сфере анализа и обработки информации, работающие с документами, презентациями, электронными таблицами и аналогичной информацией, часто используют решения, принятые на базе ПК. Другие пользователи организации частот используют Интернет технологию для приложений, таким образом предоставляя доступ к ПИУ и к сотовым телефонам.

В случае с любой конечной системой прежде всего необходимо разобраться с проблемами безопасности в операционной системе. Неиспользуемые и ненужные подсистемы, например функции базы данных и операционной системы, должны быть отключены и удалены. Другие функции должны быть ограничены до минимума, необходимого для нормальной работы пользователя. Кроме того, организация должна иметь определенный механизм использования патчей для систем и распространения обновлений по мере их поступления от поставщиков, как для операционной системы, так и для любых приложений, работающих на конечных системах.

Помимо операционной системы организация должна рассмотреть роль конечных систем и принять решение о необходимости дополнительных средств, таких, как антивирусные программы, обнаружение и предупреждение вторжения, межсетевые экраны и виртуальная частная сеть для пользователей организации. Во многих случаях внешние системы безопасности данной организации (определенные в 11.5) обеспечивают свойства, подобные антивирусным программам, межсетевым экранам, обнаружению и предупреждению вторжения. Однако при наличии мобильных систем и с ростом бизнес-партнерства и аутсорсинга для традиционной многоуровневой защиты имеет смысл дублировать эти свойства в мобильных системах и, потенциально, в ПИУ и настольных ПК. Например, мобильный ПК пользователя, подсоединенный к широкополосной связи из дома и использующий виртуальную частную сеть организации, становится каналом атаки и временным устройством периметра, требующим такой же защиты, как и другие устройства периметра.

D.1.2 Средства управления системами сервера

Подобно конечным системам системы сервера нуждаются в применении как внутренних, так и внешних средств управления на уровне операционной системы. Серверы часто нуждаются в функциональных возможностях и подсистемах, которые не требуются для конечных систем. Поскольку на сервере может использоваться база данных, веб-сервер, FTP-сервис, эти серверы имеют более значительный потенциал уязвимости. Для этих серверов требуется предоставление доступа к другим устройствам, которые не всегда заслуживают доверия. Кроме того, по мере выпуска новых патчей и версий для них, как и для конечных систем, необходимо предусмотреть условия тестирования, обновления и менеджмента систем. Примером является тестирование нового патча в непроизводственной среде перед его установкой на производственных системах.

Что касается внутреннего средства управления, сервер всегда должен использовать средства управления операционной системы, ограничивающие функции и доступ к критически важным своим частям. Это означает, например, что сервер, используемый для поддержки веб-страниц, не обязательно должен задействовать сервис FTP или открытые порты для общих запросов базы данных. Аналогично сервер FTP не должен быть открыт для портов и протоколов HTTP.

Помимо операционной системы определенное внимание необходимо уделить антивирусным программам, обнаружению вторжения и межсетевым экранам сервера и вокруг него. Эта защита может быть осуществлена в виде размещения сервера в безопасной зоне за межсетевым экраном и использования системы обнаружения вторжения на базе сетевого устройства или все три сервиса безопасности могут быть использованы на самом хосте сервера. Заинтересованность в вопросах безопасности организации и сетей служит побудительным мотивом к оценке и определению уместности тех или иных средств контроля для конкретных серверных систем.

D.1.3 Средства управления универсальными вычислительными машинами

Универсальные вычислительные машины для обработки больших объемов данных создаются лишь немногими производителями. В результате универсальные вычислительные машины рассматриваются как более надежные и более мощные, чем другие системы обработки ИТ. Тем не менее менеджмент универсальных вычислительных машин должен осуществляться посредством таких же принципов обеспечения безопасности, что и для других систем. Основная операционная система должна быть защищена, и для этого необходимо рассмотреть дополнительные меры за пределами операционной системы. Обычно универсальная вычислительная

машина хранит наиболее ценную информацию и деловой регламент, поэтому данная информация размещается в центре многоуровневой сетевой архитектуры безопасности. Каждому пользователю присваивается соответствующий идентификатор с ограниченными функциональными возможностями. Административное управление универсальной вычислительной машиной осуществляется несколькими сотрудниками. Как и в случае с другими системами, необходимо внимательно рассмотреть вариант разделения обязанностей как часть средств управления безопасностью универсальной вычислительной машины.

D.1.4 Средства управления другими аппаратными системами

Аналогичные проблемы свойственны и другим аппаратным устройствам и системам, эти проблемы необходимо решить до развертывания производства в организации. Данные устройства могут быть специальными шифровальными системами, новыми типами аппаратных средств, которым оказывают предпочтение многие поставщики межсетевых экранов и систем обнаружения вторжения, или сетевыми аппаратными средствами, например маршрутизаторами и коммутаторами. Во всех случаях продукцию необходимо оценить, чтобы иметь понятие о лежащей в его основе операционной системе — операционная система должна быть защищена от слабых атак. Кроме того, большое значение имеет расположение данных устройств по отношению к внутренним сетевым соединениям, межсетевым экранам, системам поиска вирусов и обнаружения вторжения.

D.2 Программные средства

D.2.1 Веб-серверы

Веб-серверы являются очень распространенным и часто используемым приложением, главным образом предназначенным для распределения веб-страниц для пользователей. Приложения могут варьироваться от очень простых, представляющих только фиксированные страницы информации, до очень сложных, предоставляющих многостраничные документы с поддержкой сценариев, активных программных машинных команд и т. д. Организации должны определить необходимую для них степень сложности и соответствующие связи между Интернетом, веб-сервером (веб-серверами) и внутренними данными. Обычно финансовые учреждения настаивают на трехзвенной архитектуре с межсетевыми экранами, обеспечивающими границу между Интернетом и веб-сервером и между веб-сервером и внутренними данными. Многозвенные архитектуры, разделяющие дополнительные уровни приложений или бизнес-логики, часто используются для обеспечения более жесткого управления потоками данных.

Многие поставщики распространяют программные средства веб-серверов, и каждая версия этих программных средств имеет собственную совокупность вопросов, установок и модернизаций, нуждающихся в управлении. Часто поставщик или третья сторона предлагают в Интернете связанные с безопасностью установки. Эти установки необходимо рассматривать и оценивать в соответствии с конкретными политиками, практическими приемами и потребностями определенной организации.

D.2.2 Серверы приложений и веб-сервисы

Специализированные веб-серверы стали использоваться как серверы приложений — серверы, которые могут прогонять функциональные части приложения как многократно используемые компоненты и задействоваться многими приложениями. Например, функция перемещения денежных средств между счетами может работать как компонент на сервере приложений и использоваться как приложениями, предоставляющими клиентам банковские услуги в режиме реального времени, так и операторами центра обработки вызовов, действующими от имени клиента, обращающегося за банковскими услугами. Этим компонентам приложений были приданы интерфейсы, позволяющие осуществлять вызов компонентов через веб-сервисы. Эти веб-сервисы действуют во многом аналогично более старым удаленным вызовам процедуры, но с сетевой особенностью, улучшенной использованием расширяемого языка разметки XML, который может использоваться на любых устройствах, даже на тех, которые не поддерживают традиционные веб-браузеры. Многие поставщики предоставляют серверы приложений, поддерживающие веб-сервисы. Более подробная информация о веб-сервисах и безопасности веб-сервисов представлена в приложении В.

Как и в случае с веб-серверами, многие поставщики распространяют программные средства веб-сервисов и сервера приложений, и каждая версия имеет собственный набор вопросов, установок и модернизаций, которые нуждаются в управлении. Часто поставщик или третья сторона распространяют для использования связанные с безопасностью установки в Интернете. Эти установки должны быть рассмотрены и оценены относительно конкретных политик, практических приемов и потребностей определенной организации.

D.2.3 Процесс разработки прикладных программ

Многие организации адаптируют программные средства к своим потребностям или создают специальные приложения, используя инструменты для разработки, предоставляемые крупными и мелкими поставщиками. Эти инструментальные средства разработки программного обеспечения редко приводят к внедрению информационной безопасности. Поэтому необходимо, чтобы организации планировали включение информационной безопасности в свой процесс разработки программных средств. Специалисты в области безопасности заявляют, что информационная безопасность наиболее эффективна в том случае, если требования безопасности внедряются в программное обеспечение во время разработки, а не тогда, когда программные модули безопасности защиты добавляются к законченной системе.

До начала разработки программных средств разработчики должны быть проинформированы о политике информационной безопасности организации, о том, как она связана с разработкой, и должны осознавать угрозы, направленные против организации. Разработчики должны быть осведомлены также о программе обеспечения

информационной безопасности и о том, где они могут получить рекомендации по разработке. Прочная основа в виде политики организации, ее практические приемы и постоянное сотрудничество с работниками службы обеспечения информационной безопасности будут гарантировать эффективность и результативность информационной безопасности посредством программных средств.

В разработке прикладных программ, включающих в себя требования безопасности, необходимо учитывать два аспекта. Первый заключается в том, что сам процесс разработки программных средств состоит из хорошо структурированных и документированных шагов. Целью этой разработки является создание программных средств, отвечающих исключительно собственным требованиям и не позволяющих случайно или преднамеренно выполнять нежелательные операции. Для достижения этой цели организация должна требованиям ИСО/МЭК 21827 [13]. Дополнительную информацию о модели развития функциональных возможностей можно получить на сайте gost.e-ecolog.ru. Прикладные программы с критически важными требованиями информационной безопасности должны разрабатываться с использованием процессов, определяемых уровнем 3 или более высокими уровнями модели развития функциональных возможностей, для чего требуется, чтобы процесс создания программного обеспечения для мероприятий менеджмента и проектирования был документирован, стандартизован и включен в стандартный процесс создания программного обеспечения для организации. Во всех проектах должна использоваться утвержденная, специально адаптированная версия стандартного процесса создания программного обеспечения организации для разработки и поддержки программных средств.

Вторым аспектом является включение в разработку прикладных программ соответствующих требований безопасности приложения. Эти требования формируются политикой информационной безопасности организации, архитектурой безопасности и оценкой риска. Все требования должны быть документированы, включены и протестированы во время процесса разработки. Требования безопасности должны также определять, какой объем доказательств потребуется для демонстрации полного соответствия политике безопасности и любому регулирующему законодательству.

Поскольку знание функционирования программных средств защиты данных может подвергнуть риску приложение, документация, например результаты тестирования и инструкции для оператора, должна находиться под контролем, чтобы она неумышленно не стала доступной для несанкционированного использования. Полное описание основных вопросов разработки можно найти в общедоступной публикации NIST SP800—64 «Соображения безопасности в жизненном цикле развития системы» [34], на сайте gost.e-ecolog.ru index.html.

D.2.4 Приобретение программных средств защиты данных

Организация может заключить договор с другой организацией на разработку программных средств защиты данных или приложений с учетом требований безопасности. Проблемы, определенные в D.2.3, пригодны для процесса приобретения, но в процессе разработки существуют два различия. Первое различие заключается в том, что процесс разработки ограничивается письменным договором. Внесение изменений в требования изменят договор и, вероятно, приведут к увеличению стоимости и сроков разработки. Второе различие состоит в том, что подрядчик обычно не осведомлен о структуре и культуре труда организации. Различные предположения и неправильное представление об организации будут способствовать изменениям договора. Таким образом, приобретающая организация должна быть крайне осторожной при определении требований, выборе разработчика и проведении приемочных испытаний.

Организации могут также приобретать готовые к использованию программные средства защиты данных для удовлетворения некоторых требований архитектуры безопасности. Должно существовать четкое понимание возможностей и ограничений этих программных средств. Это понимание необходимо для идентификации остаточных требований, которые будут удовлетворены другими элементами архитектуры.

Новые программные средства должны быть совместимыми с существующими программными средствами так, чтобы они не превращали в недействительные или не компрометировали существующие процедуры безопасности. Обычно используемым эталоном программных средств защиты данных являются общие критерии, представляющие собой совокупность требований и спецификаций безопасности, определенных в ИСО/МЭК 15408 [7]. В общих критериях описываются функциональные требования и требования доверия к безопасности, которые могут быть полезными для исследования требований и сравнения продуктов ИТ от различных производителей.

Общие критерии свободно доступны на сайте gost.e-ecolog.ru

D.3 Сети

D.3.1 Глобальные сети

D.3.1.1 Обзор

Глобальные сети охватывают широкие территории, используя протоколы связи, предназначенные для выхода далеко за пределы местного комплекса зданий или территории внутри здания. Интернет состоит из множества меньших глобальных сетей, каждая из которых имеет собственный набор маршрутизаторов, коммутаторов и шлюзов с другими глобальными сетями. Так называемая «обычная» телефонная сеть — это еще одна глобальная сеть. Во всех случаях глобальные сети повсюду делают возможным перемещение потока данных. Кроме того, они предоставляют множество точек доступа, где информация становится уязвимой.

В более крупных организациях, части которых расположены территориально далеко друг от друга, сеть включает в себя соединения с глобальной сетью, например, с Интернетом, посредством нескольких локальных сетей в каждом комплексе зданий или внутри здания и нескольких специальных соединений с глобальной сетью,

выделенных для организации. Обычно эти выделенные соединения с глобальной сетью считаются внутренними для организации и на них отсутствуют граничные средства управления, используемые для соединения с другими фирмами или внешними глобальными сетями, например, с Интернетом. Как часть регулярных оценок риска организации должны быть рассмотрены возможность контролирования специализированных соединений с глобальной сетью и шифрования особо ценной информации. Кроме того, должен тщательно контролироваться доступ, предоставляемый пользователям вне сети организации.

D.3.1.2 Проводные глобальные сети

Большинство глобальных сетей являются проводными, использующими оптоволоконные или медные кабели, соединяющие коммутаторы и маршрутизаторы. Как отмечалось выше, шифрование редко используется в проводных глобальных сетях, за исключением критически важных сетевых связей. Чаще кабели проводной глобальной сети защищены физически, будучи размещены внутри стен, шкафов и подвалов, куда имеют доступ немногие люди. Эти формы физической защиты и периодическая проверка соединений являются единственными мерами безопасности, связанными с большинством проводных глобальных сетей. В случае, если компания приобретает специализированные линии, может проводиться их определенное тестирование, но альтернатив основанному на договоре доверию к провайдеру телекоммуникационных услуг существует немного. Иногда проводное соединение с глобальной сетью, фактически включающее в себя линии СВЧ-связи, лазерные линии или радиочастотные линии (включая спутник), которые вводят дополнительные возможности для мониторинга информации, проходящей через глобальную сеть, даже предпочтительно.

D.3.1.3 Беспроводные глобальные сети

По мере разрастания сетей сотовой связи появляются новые системы передачи данных. Хотя большинство из них все еще являются сравнительно медленнодействующими (около 20 кбит/с), существует перспектива мегабитных передач посредством сетевых протоколов на базе сотовой телефонии. Поскольку эти системы используют мобильный характер сотовой сети и поддерживают связь при высокой пропускной способности, их часто называют системами беспроводной глобальной сети. Эти системы также обладают ограниченными возможностями по обеспечению шифрования и аналогичными возможностями обеспечения безопасности. Однако увеличивающаяся конфиденциальность многих клиентов-организаций по отношению к вопросам безопасности глобальной сети, особенно для сотовых телефонов, привела к большей «встроенной» безопасности, включая шифрование данных, по крайней мере, в отношении телефонов — см. 9.3.2.2.

D.3.2 Локальные сети

D.3.2.1 Обзор

Локальные сети распространены на территории комплекса зданий, этаже здания или даже в главном офисе. Локальные сети частот используют те же протоколы и системы маршрутизации, что и их более крупные «родственники» — глобальные сети, но обычно обеспечивают защиту, используя определенный вид шлюзов между локальной и глобальной сетями. Шлюз может быть простым агрегатом пропускной способности и маршрутизации трафика или может включать в себя межсетевые экраны, системы поиска вирусов, обнаружения вторжения и другие граничные меры управления безопасностью (см. 11.5). Во всех случаях понимание важности сетевых соединений и контроля за шлюзами является решающим аспектом обеспечения безопасности локальной сети. Другие особенности локальной сети обсуждаются ниже.

D.3.2.2 Системы проводных локальных сетей

Проводные локальные сети обычно защищены физически путем осуществления менеджмента маршрутизаторов, коммутаторов и кабельных соединений. В некоторых случаях распределение IP-адресов и другие функции менеджмента могут ограничивать возможность подключения новых устройств к локальной сети, хотя пользователи локальной сети могут посчитать столь строгий менеджмент сети очень сложным и бесполезным.

D.3.2.3 Системы беспроводных локальных сетей

D.3.2.3.1 Общая информация

Беспроводные локальные сети, особенно Wi-Fi системы или системы 802.11x, обычно обеспечивают радиочастотный сигнал для ближней связи (~100 м), который может использоваться для сетевых соединений и распределения данных. С беспроводными локальными сетями связаны многочисленные проблемы безопасности, наиболее очевидным из которых является умышленное транслирование потенциально конфиденциальной информации компании. Также возможны более изощренные атаки, берущие под контроль соединение, переадресующие трафик и связи в сети. После нескольких лет относительно безопасных решений (протокола шифрования в беспроводной связи) стали доступны открытые и совместимые стандарты для 802.11x систем. Сделанный по образцу частного стандарта безопасности Cisco под названием «Упрощенная расширяемая агентная платформа, открытый стандарт», Защищенный расширенный протокол аутентификации (PEAP) стал доступен в различных беспроводных системах. При создании любой беспроводной локальной сети в организации необходимо тщательно рассмотреть использование PEAP или сходных механизмов обеспечения безопасности.

При создании беспроводной среды существуют две основные альтернативы архитектуры. Первая состоит в использовании PEAP и обеспечении беспроводного доступа к сети только санкционированным системам и пользователям сети и создании локальной сети внутри сети организации, рассматривая всех пользователей беспроводных сетей как доверенных членов компании. Другая альтернатива — подсоединение беспроводной локальной сети, являющейся внешней для сети компании, и использование виртуальной частной сети, веб-сайтов SSL или аналогичных слоев безопасности для защиты доступа к ресурсам компании. Более подробное объяснение см. D.3.2.3.2—D.3.2.3.4.

D.3.2.3.2 Беспроводная локальная сеть в пределах организации

Компании, использующие PEAP, могут обеспечивать использование ресурсов компании и доступ только санкционированных пользователей к беспроводной локальной сети. Данное решение проблемы все еще уязвимо для атак отказа в обслуживании, но, если менеджмент и поддержка беспроводной сети в основном осуществляется внутри здания или комплекса зданий, находящихся под контролем компании, то такое решение является вполне целесообразным. Это предусматривает перемещение пользователей в границах организации — ситуация, типичная для лиц, посещающих различные совещания в разных конференц-залах, или должностных лиц, часто переезжающих между различными филиалами компании. Кроме того, такое решение ограничивает доступ к сети, Интернет-соединениям и другим ресурсам компании только этим санкционированным пользователям. Подробности безопасной реализации PEAP в этой внутренней модели архитектуры слишком многочисленны, чтобы обсуждать их подробно. Многие ресурсы предоставляются поставщиками и Интернетом.

D.3.2.3.3 Беспроводная локальная сеть за пределами организации

Альтернативой ограничения использования беспроводной сети санкционированными пользователями является предоставление беспроводного соединения с Интернет-связью, являющегося внешним для сетей организации. В этом случае пользователем беспроводного соединения может быть любой человек или лицо, абонирующее услуги. Они не будут иметь немедленного доступа к ресурсам компании. Вместо этого пользователи, которым нужен доступ к ресурсам компании, используют (см. 11.2.1) для безопасного соединения с сетью компании виртуальную частную сеть. Данному решению присущи недостатки сетевого менеджмента, однако для пользователей здесь могут быть преимущества. Финансовые учреждения обычно не желают, чтобы посторонние пользователи использовали ресурсы беспроводной локальной сети, например, университет может пожелать сделать беспроводную локальную сеть доступной для посетителей университетского городка. В качестве альтернативы университету компания управления недвижимым имуществом может захотеть сделать беспроводную локальную сеть доступной для всех арендаторов в строительном комплексе.

D.3.2.3.4 Дополнительная информация относительно беспроводной локальной сети

Во многом подобно тому, как широкополосное соединение дома делает конечную систему граничным устройством между Интернетом, сетью и ресурсами компании, беспроводная локальная сеть также преобразует конечные системы (подобные портативным компьютерам) в граничные устройства. Поэтому конечные системы, использующие беспроводные соединения, должны представляться в качестве кандидатов для применения антивирусных программ, межсетевых экранов и программных средств обнаружения вторжения, локально работающих на конечной системе.

Пользователи портативных компьютеров, соединенные с беспроводной локальной сетью, выдвигают дополнительные требования. Независимо от того, является ли беспроводная локальная сеть компании внутренней или внешней по отношению к сети организации, этим мобильным пользователям требуется доступ к ресурсам компании через виртуальную частную сеть (IPSEC либо SSL) вследствие возрастающей популярности беспроводных «горячих точек». Эти «горячие точки» располагаются в аэропортах, парках, университетах, кафетериях, ресторанах, гостиницах и других местах, часто посещаемых лицами, совершающими деловые поездки. Часто путешествующим руководителям, имеющим доступ к беспроводным сетям, повсеместно требуется связь с Интернетом. Виртуальная частная сеть предоставляет мобильному пользователю доступ к ресурсам компании, где бы он ни находился.

Основной проблемой обслуживания этих мобильных пользователей в «горячих точках» является доверие обычным интернетовским IP-адресам. Многие компании используют диапазоны 10. и 168. IP-адресов для файловых услуг и услуг печати для коллективного употребления внутри компании. Эти немаршрутизированные адреса часто используются повторно, так что домашняя сеть, сеть в кафетерии и сети во многих компаниях вместе могут использовать один и тот же адрес (например 10.1.1.100), где каждая сеть имеет различные устройства и ресурсы в этом адресе. Поскольку профили виртуальной частной сети часто определяют принятие решений о шифровании и маршрутизации на основе адреса, адреса 10. и 168. могут вызывать неоправданное доверие портативного компьютера, создавая новые потенциальные риски. Подобно виртуальной частной сети межсетевые экраны и системы обнаружения вторжения также задействованы в принятии решения о подсоединении и доверии на основе адресов. Поэтому, хотя для пользователя портативного компьютера уместно доверие к принтеру на работе и даже дома, доверие к файловому серверу в кафетерии должно быть совершенно иным. Политики, программные средства и другие меры противодействия в отношении этих проблем должны оцениваться и применяться на основе общей политики компании.

D.3.3 Дополнительная информация, связанная с телекоммуникациями

Проблемы, связанные с телекоммуникациями, существовали всегда. Продолжающееся слияние речи и данных в одних и тех же сетях открывает новый ряд проблем для телекоммуникаций и мер противодействия. Недавно разработки речевых межсетевых экранов, магистральных виртуальных частных сетей и мультимедийных систем обнаружения вторжения, которые рассматривают проблемы слияния данных/речи, начали реализовываться в виде продукции и серьезно рассматриваться крупными поставщиками. Эти разработки также реализуются компаниями и часто окупаются экономически в результате более качественного управления речевыми телекоммуникациями в пределах компании.

Приложение Е
(справочное)

Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам

Таблица Е.1

Обозначение ссылочного международного стандарта	Обозначение и наименование соответствующего национального стандарта
ИСО 9564	*
ИСО 10202	*
ИСО 11568	*
ИСО/МЭК 11770	*
ИСО 15782	*
ИСО 16609	*
ИСО/МЭК 17999:2000	ГОСТ Р ИСО/МЭК 17799—2006 «Информационная технология. Методы обеспечения безопасности. Руководство по управлению безопасностью информации»
ИСО/МЭК 18028-4	*
ИСО/МЭК 18033	*
ИСО 21188:2006	*
* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта.	

Библиография

[1] ИСО 7498-2:1989 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации

[2] ИСО/МЭК 13335-1:2004 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

[3] ИСО 15782-1:2003 Управление выдачей сертификатов для финансовых услуг

[4] ИСО/МЭК 10181-1:1996 Информационная технология. Взаимосвязь открытых систем. Структуры обеспечения безопасности открытых систем. Часть 1. Обзор

[5] ИСО/МЭК ТО 13335-4:2000 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

[6] ANSI X9.84:2003 Управление биометрической информацией и безопасностью в области финансовых услуг

[7] CPSS Ключевые принципы для системно значимых платежных систем

[8] ANSI X9.79:2001 Структура практических приемов и политика инфраструктуры открытых ключей в области финансовых услуг

[9] ИСО/МЭК 13888-1:2004 Информационная технология. Способы и методы обеспечения безопасности. Неотказуемость

[10] Соглашение Базель II Банка международных расчетов (BIS — см. http:/gost.e-ecolog.ru)

[11] Закон Сэрбэйнс-Оксли (SOX)

[12] «Gramm-Leach-Bliley (GLB) Act of 1999, gost.e-ecolog.ru

[13] Европейская директива 95/46/EC

[14] Швейцарский закон о защите данных

[15] Закон о тайне вкладов клиентов швейцарского банка (Schweizer Bankkundengeheimnis)

[16] Директива ЕС 82/121/ЕЭС

[17] Директива ЕС 2000/31/EC (об электронной торговле)

[18] Закон Kreditwesengesetz (KWG)

[19] Ключевые принципы Банка международных расчетов (gost.e-ecolog.ru)

[20] ИСО/МЭК 13335-2:1997 Информационная технология. Методы и средства обеспечения безопасности. Часть 2. Управление и планирование безопасности информационных технологий

[21] ИСО/МЭК 13335-3:2004 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

[22] ИСО 21188:2006 Инфраструктура открытого ключа для финансовых услуг. Практические приемы и основы политики

[23] «Рекомендации по управлению паролями Министерства обороны США» от 12 апреля 1985 г. (CSC-STD-002—85)

[24] Сайт gost.e-ecolog.ru

[25] ИСО 19092:2008 Финансовые услуги. Биометрика. Схема защиты.

[26] FIPS 140-2:2001 Требования безопасности для криптографических модулей. Национальный институт стандартов и технологий США, gost.e-ecolog.ru

[27] ИСО/МЭК 18043:2006 Информационная технология. Развертывание и эксплуатация систем обнаружения вторжений

[28] ИСО 9564 Управление и обеспечение безопасности личного идентификационного кода

[29] ИСО ТО 19038:2005 Банковское дело и связанные с ним финансовые услуги. Тройной алгоритм шифрования данных. Рабочий режим. Рекомендации по внедрению

[30] ANSI X9.52:1998 Режим эксплуатации тройного алгоритма шифрования данных

[31] FIPS 197:2001 Усовершенствованный стандарт шифрования (AES). Национальный институт стандартов и технологии США

[32] Заявление Института внутренних аудиторов.

[33] ИСО/МЭК 18044:2004 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности

[34] Публикации NIST SP800—64 «Соображения безопасности в жизненном цикле развития системы», на сайте gost.e-ecolog.ru

[35] ИСО/МЭК 19790:2006 Информационная технология. Способы и методы обеспечения безопасности. Требования безопасности криптографических модулей

УДК 004.056:006.354 ОКС 01.040.01
35.040 Т00

Ключевые слова: финансовые услуги, информационная безопасность, событие информационной безопасности, система менеджмента информационной безопасности

Редактор *В. Н. Копысов*
Технический редактор *Н. С. Гришанова*
Корректор *С. В. Смирнова*
Компьютерная верстка *Т. Ф. Кузнецовой*

Сдано в набор 14.11.2008. Подписано в печать 16.02.2009. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 7,44. Уч.-изд. л. 8,00. Тираж 288 экз. Зак. 2590.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано и отпечатано в Калужской типографии стандартов, 248021 Калуга, ул. Московская, 256.
gost.e-ecolog.ru