Экз. № ___

**Федеральное агентство по техническому регулированию и метрологии**

Логотип национального органа по стандартизации

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ГОСТ Р ИСО/МЭК 13569-**

*(проект, первая редакция, 10.05.2007)*

**Финансовые услуги**

# РЕКОМЕНДАЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**ISO/IEC TR 13569:2005**

# Financial services — Information security guidelines

**(IDT)**

**Настоящий проект стандарта не подлежит применению до его принятия**

**Москва**

# 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 п. 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 "___" _____ 200_ № _____

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

Распространение настоящего стандарта на территории Российской Федерации осуществляется с соблюдением правил, установленных Федеральным агентством по техническому регулированию и метрологии

## Содержание

# Введение

Финансовые бизнес-практики изменились с внедрением компьютерных и сетевых технологий. Возросшая зависимость от электронных операций усилила потребность в осуществлении менеджмента безопасности информационно-коммуникационной технологии. Большие суммы в виде денежных средств и ценных бумаг переводятся ежедневно с помощью механизмов электронной связи, контролируемых практическими приемами обеспечения безопасности, которые основаны на политиках бизнеса.

Высокая стоимость и большие объемы таких операций во все более взаимосвязанной и открытой среде подвергают финансовую индустрию опасности потенциально серьезных последствий. Взаимосвязанные сети и возрастающие число и опыт нарушителей объединяют этот риск с вероятностью воздействия на банки и их клиентов. А когда финансовые операции включают системно значимые платежные системы, эти последствия могут оказать неблагоприятное влияние на национальный и мировой финансовые рынки.

Необходимость расширения бизнес-операций в этой среде и менеджмент риска требует серьезной и эффективной программы обеспечения информационной безопасности предприятия. Финансовые учреждения должны руководить этими программами всесторонним образом, так же как они осуществляют менеджмент рисков посредством хорошо обоснованных бизнес-практик и бизнес-соглашений, осмотрительного привлечения внешних ресурсов для определенных функций, страхования и использования соответствующих защитных мер. Они должны также разрабатывать свои программы обеспечения безопасности для рассмотрения изменяющихся рисков и требований, обусловленных развивающейся национальной и международной правовой и нормативной средой.

Как предупреждают нас Базельские соглашения, операционный, и правовой риски могут вызывать или усиливать кредитный риск и риск ликвидности. Менеджмент этих рисков становится главным для программы обеспечения информационной безопасности финансового учреждения. Чтобы понимать их воздействие, каждое финансовое учреждение должно интерпретировать эти риски с точки зрения собственной бизнес-деятельности,. Следует уделять тщательное внимание операционным рискам, включая мошенническую и преступную деятельность, природные бедствия и террористические акты. События, имеющие низкую степень вероятности, такие как цунами, обрушившееся на Азию в декабре 2004 года, и террористические атаки 11 сентября 2001 года на финансовые службы в Нью-Йорк Сити, все-таки происходят и должны предусматриваться.

Данный Технический Отчет предназначен для использования финансовыми учреждениями различного масштаба и типа, которые должны применять разумную и коммерчески обоснованную программу менеджмента информационной безопасности. Он также содержит полезные рекомендации для поставщиков услуг финансовым учреждениям, и может служить в качестве первоисточника для преподавателей и издателей, обслуживающих финансовую индустрию.

Целями данного Технического Отчета является следующее:

– определение программы менеджмента информационной безопасности;

– представление организации и политики программы и необходимых структурных компонентов;

– представление рекомендаций по выбору средств обеспечения безопасности, представляющих собой принятые разумные бизнес-практики в финансовых услугах;

– информирование руководства финансовых организаций о необходимости систематического рассмотрения правовых рисков в его программе менеджмента информационной безопасности.

Данный Технический Отчет не предназначен для предоставления единого общего решения для всех учреждений, предоставляющих финансовые услуги. Каждая организация должна проводить анализ риска и выбирать соответствующие действия. Данный Технический Отчет предоставляет рекомендации для проведения такого процесса, а не предлагает конкретные решения.

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ**

---

**Финансовые услуги**

**РЕКОМЕНДАЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Financial services
Information security guidelines

---

**Дата введения 200X-XX-0X**

# 1 Область применения

Данный Технический Отчет предоставляет рекомендации по разработке программы обеспечения информационной безопасности для учреждений в индустрии финансовых услуг. Он включает обсуждение политик, организации, а также структурных, правовых и нормативных компонентов программы. Обсуждаются соображения, касающиеся выбора и внедрения средств обеспечения безопасности и элементы, необходимые для осуществления менеджмента рисков информационной безопасности в современном учреждении по предоставлению финансовых услуг. Приводимые рекомендации основываются на рассмотрении бизнес-среды, практических приемов и процедур финансовых учреждений. В данные рекомендации включено обсуждение проблем правового и нормативного соответствия, которые должны учитываться при проектировании и внедрении программы.

# 2 Нормативные ссылки

Следующие упомянутые документальные источники необходимы для применения данного документа. В случае документов с обозначенной датой применимы только упоминаемые издания. Для документов без обозначенной даты применимо последнее издание упомянутого документа (включая любые поправки).

ИСО 9564 (все части), *Банковское дело – Менеджмент личного идентификационного номера (PIN) и обеспечение безопасности*

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 для финансовых услуг*

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

ИСО/МЭК 17799*, Информационная технология – Методы и средства обеспечения безопасности – Кодекс установившейся практики для менеджмента информационной безопасности*

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, *Инфраструктура открытых ключей для сферы финансовых услуг – Практические приемы и структура политики*

П р и м е ч а н и е – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов и классификаторов в информационной системе общего пользования – на официальном сайте национального органа Российской Федерации по стандартизации в сети Интернет или по ежегодно издаваемому информационному указателю "Национальные стандарты", который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании настоящим стандартом, следует руководствоваться замененным (измененным) стандартом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

# 3 Термины и определения

В настоящем стандарте используются следующие термины с соответствующими определениями.

**3.1 управление доступом** (access control): Функции, ограничивающие доступ к информации или средствам обработки информации только тем лицам или приложениям, которые санкционированы на такой доступ, включая физическое управление доступом, основанное на размещении физических барьеров между несанкционированными лицами и защищаемыми информационными ресурсами, и логические средства управления доступом, использующие другие способы.

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

[ИСО 7498-2; ИСО/МЭК 13335-1:2004, определение 2.1]

**3.3 звуковое предупреждение** (accountability): Указание на нарушение безопасности, необычное или опасное состояние, которое может потребовать немедленного внимания.

**3.4 активы** (alarm):Все, что имеет ценность для организации.

[ИСО/МЭК 13335-1:2004, определение 2.2]

**3.5 аудит** (audit):Функция, которая стремится подтвердить достоверность наличия мер управления и их соответствия своему назначению, и которая сообщает руководству соответствующего уровня о несоответствиях.

**3.6 журнал регистрации** (audit journal): Запись в хронологическом порядке действий системы, которых достаточно, 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, определение 3.3]

**3.7 аутентификация** (authentication): Обеспечение уверенности в заявленной идентичности логического объекта.

[ИСО/МЭК 10181-2, ИСО/МЭК TR 13335-4:2000, определение 3.1]

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

П р и м е ч а н и е — Аутентичность применяется к таким субъектам, как пользователи, к процессам, системам и информации.

**3.9 доступность** (availability): Свойство, объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта.

[ИСО 7498-2, ИСО/МЭК 13335-1:2004, определение 2.4]

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

**3.11 биометрические данные** (biometric): Измеримая биологическая или поведенческая характеристика, с надежностью отличающая одного человека от другого, которая используется для распознания личности или подтверждения заявленной личности человека.

[ANSI X9.84:2003]

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

**3.13 аутентификация карточек (МАК)** (card authentication methodCAM): Понятие, делающее возможной уникальную машиночитаемую идентификацию банковской карточки для финансовых операций и предотвращающее копирование карточек.

**3.14 классификация** (classification): Схема, разделяющая информацию на категории, такие как: возможность мошенничества, конфиденциальность или критичность информации, с целью возможности применения соответствующих защитных мер.

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

[ИСО 7498-2, ИСО/МЭК 13335-1:2004, определение 2.6, ИСО/МЭК 15782-1:2003, определение 3.19]

**3.16 план действий в чрезвычайных обстоятельствах** (contingency plan): Процедура, которая, в случае следования ей, позволяет организации восстановить работу после природного или иного бедствия.

**3.17 мера управления** (control): Смотри определение понятия "защитная мера".

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

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

[CPSS, Ключевые принципы для системно значимых платежных систем]

**3.20 критичность** (criticality): Требования в отношении того, чтобы определенная 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 ИСО 16609, с криптографическим ключом, распределяемым в соответствии с ИСО 11568, или выводимая из успешного дешифрования сообщения, зашифрованного в соответствии с ИСО 18033 (в соединении с ИСО/TR 19038 или ANSI X9.52), с ключом, операции с которым осуществляются в соответствии с ИСО/МЭК 11770.

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

П р и м е ч а н и е. Знание соответствующего ключа дает возможность правильно дешифровать или подтверждать целостность сообщения.

**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]

**3.26 раскрытие информации** (disclosure of information): Несанкционированный просмотр или потенциальный просмотр информации.

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

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, передачи, загрузки, хранения и извлечения ключей и сертификатов двойной контроль требует раздельного знания ключа логическими объектами.

3. Когда бы ни требовался двойной контроль, следует позаботиться о том, чтобы обеспечить независимость лиц друг от друга.

Смотри также разделенное знание.

[ИСО 15782-1:2003, определение 3.31]

**3.28 шифрование** (encryption): Процесс преобразования информации, осуществляемый для того, чтобы привести ее в вид, непонятный для всех, 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, помещаемых между двумя сетями, которые вместе обладают следующими свойствами:

– весь сетевой трафик изнутри наружу и наоборот должен проходить через межсетевой экран;

– разрешается проходить только санкционированному сетевому трафику, как определяется местной политикой безопасности;

– межсетевой экран сам по себе устойчив к проникновению.

**3.30 идентификация** (identification): Процесс однозначного определения уникального идентификатора логического объекта

[ИСО/МЭК TR13335-4:2000, определение 3.2]

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

**3.32 инцидент информационной безопасности** (incident): Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Примечание - Инцидентами информационной безопасности являются:
- 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.

[ИСО/МЭК 13335-1:2004, определение 2.10]

**3.33 средства обработки информации** (information processing facility): Любая система обработки информации, сервис или инфраструктура, или их физические места размещения.

[ИСО/МЭК 13335-1:2004, определение 2.13]

**3.34 информация** (information): Любые данные, являются ли они представленными в электронной форме, написанными на бумаге, высказанными на собрании или находящимися на любом другом носителе, которые используются финансовой организацией для принятия решений, перемещения денежных средств, установления ставок, предоставле-

ния ссуд, обработки операций и тому подобного, включая компоненты программного обеспечения системы обработки.

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

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

[ИСО/МЭК 13335-1:2004, определение 2.14]

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

**3.38 информационные ресурсы** (information resource): Оборудование, используемое для обработки, передачи или хранения информации, такое как телефоны, факсимильные аппараты и компьютеры, независимо от того, находится ли оно внутри или за ее пределами.

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

[ИСО/МЭК 13335-1:2004, определение 2.15]

**3.40 ключ** (key): Смотри Криптографический ключ.

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

**3.42 правовой риск** (legal risk): Риск потерь из-за неожиданного применения закона или постановления или из-за невозможности выполнения контракта.

[CPSS, Ключевые принципы для системно значимых платежных систем]

**3.43 гарантийное письмо** (letter of assurance): Документ, излагающий защитные меры информационной безопасности, которые имеются для защиты информации, хранимой в интересах 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.

[CPSS, Ключевые принципы для системно значимых платежных систем]

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

П р и м е ч а н и е. 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 сообщения** (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.

[ИСО/МЭК 13888-1; ИСО 7498-2; ИСО/МЭК 13335-1:2004, определение 2.16]

**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.

[CPSS, Ключевые принципы для системно значимых платежных систем]

**3.51 обладатель информации** (owner of information): Работник или должностное лицо, которые отвечают за сбор и сохранение данной совокупности информации.

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

**3.53 разумная 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.

[ИСО/МЭК 13335-1:2004, определение 2.17]

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

[ИСО/МЭК 13335-1:2004, определение 2.18]

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

Примечание - Определяется как сочетание вероятности события и его последствий.

[ИСО/МЭК 13335-1:2004, определение 3.19]

**3.57 принятие риска** (risk acceptance): Утвержденный риск, связанный с исключением в политике.

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

[ИСО/МЭК 13335-1:2004, определение 2.20]

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

[ИСО/МЭК 13335-1:2004, определение 2.21]

**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 опасных событий, которые могут оказать влияние на ресурсы информационно-телекоммуникационых технологий.

[ИСО/МЭК 13335-1:2004, определение 3.22]

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

**3.64 защитная мера** (safeguard): Сложившиеся практические приемы, процедура или механизм обработки риска.

Примечание - Следует заметить, что понятие "защитная мера" может считаться синонимом понятию "мера управления".

[ИСО/МЭК 13335-1:2004, определение 2.24]

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

Примечания:

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

2. В рамках системы безопасности "состояние-модель" безопасность является определенным "состоянием", которое должно сохраняться при различных операциях.

**6.66 сервер** (server): Компьютер, действующий как поставщик некоторых услуг, таких как обработка коммуникаций, интерфейс файловой памяти или печатное устройство для других компьютеров.

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

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

Примечание. Разделенное знание часто используется для осуществления двойного контроля.

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

**6.70 системный риск** (systemic risk): Риск того, что неспособность одного из участников выполнить свои обязательства или нарушения в функционировании самой системы могут привести к неспособности других участников системы или других финансовых учреждений в других частях финансовой системы выполнять свои обязательства при наступлении срока платежа.

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

[CPSS, Ключевые принципы для системно значимых платежных систем]

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

[ИСО/МЭК 13335-1:2004, определение 2.25]

**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, которая используется для однозначной идентификации каждого пользователя системы.

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

[ИСО/МЭК 13335-1:2004, определение 2.26]

# 4 Обозначения и термины, приведенные в сокращении

**ATM**
Банкомат
**CEO**
Главный исполнительный директор
**CFO**
Главный финансовый директор
**CIO**
Главный директор по информационным технологиям
**CISO**
Директор по информационной безопасности корпорации

**COO**
Главный операционный директор
**CPSS**
Комитет по платежным и расчетным системам

**CTO**
Главный технический директор
**DMZ**
Демилитаризованная зона
**EFT**
Электронный перевод средств
**FTP**
Протокол передачи файлов
**HTTP**
Протокол передачи гипертекста
**HTTPS**
Протокол защищенной передачи гипертекста
**ICT**
Информационно-коммуникационные технологии
**IDS**
Система обнаружения вторжений
**IP**
Протокол Интернет
**IPSEC**
Протокол IPSec
**ИТ**
Информационная технология
**LAN**
Локальная сеть
**LEAP**
Упрощенная расширяемая агентная платформа
**MAC**
Код аутентификации сообщений
**ОС**
Операционная система
**ПК**
Персональный компьютер
**PDA**
Персональный цифровой секретарь
**PEAP**
Защищенный расширяемый протокол аутентификации
**PIN**
Личный идентификационный номер
**POTS**
Обычная телефонная сеть
**RF**
Радиочастота
**SMTP**
Простой протокол электронной почты
**SSH**
Вид терминального доступа к серверному компьютеру с большей степенью защищенности сеанса связи
**SSL**
Протокол защищенных сокетов
**USB**
Универсальная последовательная шина

**VPN**
Виртуальная частная сеть
**VTAM**
Виртуальный телекоммуникационный метод доступа
**WAN**
Глобальная сеть
**Wi-Fi**
Стандарт Wi-Fi на беспроводную связь
**WS**
Веб-сервисы
**XML**
Расширяемый язык разметки

# 5 Политика информационной безопасности организации

## 5.1 Назначение

Все учреждения финансовых услуг сегодня в значительной степени зависят от использования информационной технологии (ИТ) и информационно-коммуникационных технологий (ИКТ) и, следовательно, нуждаются в обеспечении защиты информации и менеджменте безопасности своих информационных активов. Обеспечение информационной безопасности, и менеджмент информационной безопасности должны стать важным компонентом плана менеджмента в организации для выполнения руководством своих обязанностей.

Разработка программы обеспечения информационной безопасности является разумной бизнес-практикой, которая поможет учреждениям финансовых услуг идентифицировать и осуществлять менеджмент риска. Данный Технический Отчет предлагает общий, основанный на политике подход к менеджменту информационной безопасности и представляет рекомендации, которые могут быть приспособлены для соответствия бизнес-целям организации. Бизнес-целям должны способствовать политики и процедуры для обеспечения защиты активов ИТ. Основанный на политике подход применим к учреждениям разной величины, с различными стилями управления и разными организационными средами.

Данный Технический Отчет предназначен для предоставления рекомендаций – а не конкретных решений – по аспектам менеджмента информационной безопасности и для оказания содействия руководству учреждения финансовых услуг в разработке и поддержке программы обеспечения информационной безопасности. Другие упоминаемые источники, особенно ИСО/МЭК 17799, предоставляют важную подробную информацию общего назначения, которая окажет неоценимую помощь в вопросе внедрения и поддержки. Однако в данном Техническом Отчете обращается внимание на особые правовые и нормативные требования, которые должны учитываться финансовыми учреждениями при создании основанной на политике программы менеджмента информационной безопасности.

## 5.2 Правовое и нормативное соответствие

### 5.2.1 Общая информация

Нормативные 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, закон Сэрбэйнс-Оксли (SOX), закон Грэма-Лича-Блили (GLB) [22] и Европейская директива 95/46/EC, определили среду правового и нормативного риска для мировых поставщиков финансовых услуг. Политика безопасности организации должна учитывать этот тип риска.

Служащие по обеспечению соответствия должны работать вместе с руководителем службы по информационной безопасности организации, финансовым директором, управляющими делами, лицами, занимающимися менеджментом риска, и аудиторами над обеспечением того, чтобы требования информационной безопасности, выведенные из национальных и международных законов и положений, были рассмотрены и понятны. Служащие по обеспечению соответствия должны также оставаться в курсе новых технологий или методологий, которые могут стать объектом регулирования, например, соответствие заранее определенным классам функциональных возможностей для продукции информационной технологии.

### 5.2.2 Требования к финансовым учреждениям

#### 5.2.2.1 Обзор

Для учреждений финансового сектора существуют некоторые правовые и нормативные требования, которые оказывают влияние на безопасность ИТ и должны соблюдаться. Неотъемлемая проблема состоит в том, что эти требования различаются в разных странах. Хотя Европейский Союз проложил путь к правовому выравниванию, все еще существуют национальные положения, требующие особого внимания.

В приведенном ниже рассмотрении в каждом подпункте будет описываться наиболее важные законы с точки зрения поставщика финансовых услуг, действующего в глобальных условиях. Описание законодательной среды разбито на три раздела: организационное управление, защита данных (неприкосновенность частной жизни) и законодательство финансового сектора, характерное для поставщиков финансовых услуг (например, законы, касающиеся отмывания денег). Описание нормативной среды сосредоточено на требованиях финансовой отчетности и рекомендациях соглашения Базель II, которые можно получить на сайте Банка международных расчетов [19], Базель, Швейцария, http://www.bis.org/bcbs/publ.htm.

#### 5.2.2.2 Правовые требования

##### 5.2.2.2.1. Руководство организации

В последние годы многие национальные и региональные законодательные органы выдвинули законы, рассматривающие вопрос руководстве организации. Среди них известны следующие: закон Сэрбэйнс-Оксли (SOX) в Соединенных Штатах, закон Kontrolle und Transparenz Gesetz (KonTraG) в Германии и проект директивы Европейского Союза о Руководстве .Организации. Эти три закона изменили панораму правовых рисков, с которыми сталкиваются поставщики финансовых услуг.

Закон Сэрбэйнс-Оксли требует, чтобы все компании, ведущие свободную торговлю на фондовых биржах США, предоставляли свидетельство того, что у них имеются адекватные средства контроля, для финансовой отчетности. Говоря более подробно, закон Сэрбэйнс-Оксли обязывает главного исполнительного директора и финансового директора такой компании производить оценку эффективности внутренней системы контроля организации, а также четко подписывать и принимать на себя ответственность за ежегодные финансовые отчеты организации. В отношении ИТ для этого требуется, осуществление оценки и контроля функционирования критических бизнес-приложений и связанных с ними рисков. Подводя итоги, весь жизненный цикл таких приложений – от первоначальной разработки до обеспечения непрерывности бизнеса – должен оцениваться и контролироваться, чтобы гарантировать наличие адекватных защитных мер. Хотя этот закон яв-

ляется национальным по своему происхождению, он применим к любой компании, чьи акции свободно продаются в США.

Немецкий закон Kontrolle- und Transparenz Gesetz (KonTraG) требует от организации внедрения внутреннего процесса мониторинга, определяющего внутренние разработки и решения, которые могут представлять высокий уровень риска для этой организации. Неявным образом это означает, что руководство должно внедрять внутреннюю систему менеджмента риска в масштабе организации. Он 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 и в законе Сэрбэйнс-Оксли. Однако, поскольку немецкие компании, ведущие свободную торговлю, имеют двухуровневый совет директоров, это вводит в действие более строгую систему отчетности совета директоров наблюдательному совету. Несоответствие этому закону может приводить к снижению банковского рейтинга организации и, следовательно, может оказывать влияние на процентные ставки за кредиты.

Европейский Союз (ЕС) разрабатывает проект директивы, которая окажет влияние на национальное законодательство ЕС: от всех компаний, чьи акции зарегистрированы на фондовой бирже, требуется публикация отчета о управлении организации. Этот отчет должен содержать подробности о совете директоров, его решениях, финансовом положении и соблюдении национального законодательства. Этот отчет должен также включать результаты независимых аудитов. Эта директива имеет похожие следствия для ИТ, что и у законов Сэрбэйнс-Оксли и Kontrolle- und Transparenz Gesetz (KonTraG). Существуют и другие национальные законы, охватывающие эту тему, 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, национального и государственного уровня. Эти законы инициированы тем, что Интернет и его использование представляют дополнительные риски, касающиеся злоупотребления в этой сфере, и что люди, использующие эту среду, нуждаются в соответствующей защите.

Закон Грэма-Лича-Блили (GLB) предназначен для защиты информации потребителей, хранимой финансовыми учреждениями. Он требует, чтобы эти учреждения предоставляли своим клиентам уведомление о неприкосновенности частной жизни, объясняющее практические приемы учреждений в отношении коллективного использования информации. В свою очередь потребители имеют право ограничить некоторое – но не все – коллективное использование своей информации. Закон также требует, чтобы финансовые учреждения защищали информацию, собранную об отдельных лицах; он не относится к информации, собранной в ходе коммерческой или бизес-деятельности. Федеральная торговая комиссия (FTC) опубликовала набор стандартов, который должен применяться для обеспечения соответствия закону Грэма-Лича-Блили.

Европейская директива 95/46/ЕС представляет собой совместное усилие по достижению неприкосновенности частной жизни для всех стран-участниц на высоком уровне. Она защищает информацию о физических лицах во время всего жизненного цикла обработки. Проще говоря, она требует, чтобы учреждение запрашивало разрешения в случае, если информация используется образом, отличным от официального предназначения (и заявления). Она также ограничивает передачу данных теми странами, где обеспечивается адекватная защита данных. В общем, физические лица должны давать явное разрешение (на участие), чтобы разрешить дальнейшую обработку. Это противоречит процедуре в США, где физических лиц запрашивают об отказе от участия с целью запрещения дальнейшей обработки. Эта директива внедряется в национальное законодательство во всех странах-членах ЕС.

Швейцарский закон о защите данных сходен с законами, существующими в других европейских странах. Он упоминается здесь по двум причинам: Швейцария не является частью Евросоюза и, следовательно, он должен быть упомянут. С другой стороны, швейцарский закон запрещает передачу личных данных в другие страны при отсутствии адекватной защиты, и требует от передающей организации информировать правовой орган о передаче. Другим важным законом, связанным с финансовыми учреждениями, является закон о тайне вкладов клиентов швейцарского банка (Schweizer Bankkundengeheimnis), обеспечивающий безусловную защиту информации о клиентах, хранимой банками.

**5.2.2.2.3. Отмывание денег**

Почти все страны имеют какие-либо законы по отмыванию денег, которые обычно означают, что перевод денег, превышающий определенную сумму, должен быть изучен для проверки его источников и адресата. Еще в 1990-х годах такие законы не имели бы явного отношения к безопасности, так как они могли быть внедрены в действие независимо от каких-либо вопросов безопасности.

Террористические атаки, совершенные в США 11 сентября 2001 года, ясно показали важность законов, направленных против отмывания денег, и связанных с ними мер управления.. Эти атаки стимулировали даже большее осознание важности сотрудничества в сфере борьбы с отмыванием денег по всему миру. Это осознание оживило международное сотрудничество и привело к значительным изменениям законов, направленных против отмывания денег, которые вносят свой вклад в способность мирового сообщества отслеживать денежные средства тех, кто финансирует международный терроризм.

С 2001 года Соединенные Штаты продолжают энергичную межведомственную международную обучающую программу по борьбе с отмыванием денег, чтобы улучшить международные усилия по борьбе с отмыванием денег и финансовыми преступлениями. Другие правительства и международные организации тоже усилили свои программы, направленные против отмывания денег. Европейский Союз расширил свою директиву по борьбе с отмыванием денег и наложил направленные против отмывания денег обязательства на "гейткиперов", профессионалов, таких как юристы и бухгалтеры, которые способствуют вложению "грязных денег" в финансовую систему. Продолжают эффективно работать региональные организации по борьбе с отмыванием денег в Европе, Азии и странах Карибского бассейна и начинают действовать зарождающиеся региональные организации по борьбе с отмыванием денег в Южной Америке и Африке.

Главное внимание в сфере борьбы с отмыванием денег в этом году сосредоточилось на работе Финансовой оперативной группы (FATF), всемирно признанной многосторонней организации по борьбе с отмыванием денег, которая продолжила свою работу с несотрудничающими странами и территориями. После 11 сентября 2001 года FATF быстро среагировала и созвала чрезвычайное пленарное совещание по вопросу финансирования терроризма, которое приняло решение расширить свою задачу за рамки борьбы с отмыванием денег и сосредоточить свою энергию и опыт на мировых усилиях по борьбе с финансированием терроризма. С этого времени FATF приняла восемь специальных рекомендаций по вопросу финансирования терроризма.

Террористические атаки послужили сильным толчком многим странам к внесению изменений в законы по борьбе с отмыванием денег и их усилению. В Соединенных Штатах закон об объединении и укреплении Америки путем обеспечения соответствующих средств, необходимых для препятствования терроризму от 2001 года ("USA PATRIOT") внес значительные изменения в систему борьбы с отмыванием денег в США. 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 отмывания денег. И что более важно, эти программы могут использоваться для демонстрации правоприменяющими организациями, что финансовое учреждение соблюдает соответствующее законодательство, и предоставить документацию, о том, что он систематически и активно принимает меры для соблюдения законодательства.

#### 5.2.2.2.4. Законы, касающиеся финансовых рынков

Большинство законов, регулирующих финансовый сектор, в основном определяет обязанности финансового учреждения. Это включает в себя обязательство по предоставлению квалифицированных услуг. Некоторые органы федеральной власти интерпретируют это обязательство таким образом, что оно распространяется на всю полноту используемых услуг ИТ. Следующие национальные законы указывают на конкретные вопросы безопасности ИТ.

По аргентинскому банковскому законодательству, финансовые учреждения должны включать в свой состав руководителя службы обеспечения информационной безопасности (ISO), который предоставляет ежегодный отчет центральному банку Аргентины. Отчет должен отражать, как устанавливаются и осуществляются внутренние меры управления финансового учреждения для обеспечения надлежащих услуг.

Директива Евросоюза 82/121/ЕЭС регулирует отчетность финансовых учреждений. Она была недавно обновлена для осуществления более регулярной отчетности на всей территории Евросоюза. Директива Евросоюза 2000/31/ЕС (об электронной торговле) предписывает правовую структуру для электронной торговли, которая среди прочего должна включать в себя вопросы неприкосновенности частной жизни клиентов, регулирование вопросов спама, налогообложение, электронные контракты и их обработку, конфиденциальность передачи информации. Она также определяет кодекс поведения, как средство обмена информацией о правах, задействованных экономических объектов.

Немецкий закон Kreditwesengesetz (KWG) регулирует практически все вопросы, характерные для финансовых учреждений в Германии. Он определяет, как должны функционировать банки, кому разрешается возглавлять финансовое учреждения, что должно содержаться в отчетности и т.д. Три параграфа этого закона представляют особый интерес. В первом, рассматривается проблема автоматического доступа к данным клиентов финансовым органам (§ 24c), который требует наличия дополнительных мер безопасности. Во втором, (§ 25a) определяются особые обязательства, которые должны выполнять финансовое учреждение, охватывающие такие вопросы, как менеджмент внутреннего риска, меры безопасности и внутренний аудит, а также его сотрудничество с надзорными органами. Наконец, существуют предписания на случай невыполнения финансовым учреждением или его руководством своих обязательств, что может привести к тому, что руководство утратит право ведения бизнеса в финансовом секторе.

#### 5.2.2.3 Нормативные требования

Две темы нормативных требований к финансовым учреждениям являются здесь очень актуальными. Первая тема касается обязательств учреждения по финансовой отчетности (обычно надзор осуществляется национальными финансовыми органами). Второй темой является обязательство финансовой устойчивости, которое описывается в соглашениях Базель II Банка международных расчетов (BIS – смотри http://www.bis.org/bcbs/index.htm). Эти требования включают в себя необходимость рассмотрения финансовым учреждением операционных рисков.

Базельский комитет по банковскому надзору формулирует широкие рекомендации, касающиеся стандартов, принципов и лучших практических приемов надзора. Комитет надеется, что национальные финансовые органы предпримут шаги по внедрению этих

рекомендаций посредством подробных мероприятий – предусмотренных законом или иным способом – которые лучше всего соответствуют их национальным системам. Нормативные требования приводят к необходимости проведения аудита финансовых учреждений. Для ограничения нарушений, которые могут причинять аудиты обычным бизнес-операциям, финансовые учреждения должны ввести системы (внутреннего аудита, менеджмента информационной безопасности и т. д.), которые без труда предоставят нормативным органам все необходимое для проверки, чтобы удостовериться, что финансовое учреждения соответствует требованиям.

Каждое финансов учреждение должно интерпретировать "операционный риск" в показателях собственной бизнес-деятельности и определить риски, которым оно подвергается. Анализ операционных рисков должен включать в себя мошенничество и преступную деятельность, сбои системы, человеческий фактор, природные бедствия и террористические акты. Цунами, вызвавшее большие человеческие жертвы и разрушения в Азии в декабре 2004 года, и террористические атаки в сентября 2001 года, нацеленные на индустрию финансовых услуг в Нью-Йорк Сити, являются примерами событий с крайне низкой степенью вероятности. Но такие события случаются и должны приниматься во внимание.

Соглашение "Базель II" настаивает на необходимости 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 непредвиденного обстоятельства, его вероятную частоту, прогнозируемые потери и влияние на бизнес-операции в случае, наступления события.

Отметьте, что существует 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 соглашениях Базель II, а на Ключевых принципах Банка международных расчетов (смотри http://www.bis.org/publ/bcbs49b.pdf), которые направлены на системно значимые платежные системы. Платежные системы, которые классифицируются как "системно значимые" для благополучия и нормальных операций финансовых рынков, 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 как рекламный момент, так как соответствие рассматривается как мера качества.

### 5.3 Разработка

После определения целей информационной безопасности организации и оценки воздействия положений и законодательства необходимо разработать план действий, согласующийся с установленными бизнес-целями. План должен использоваться как "путеводитель" для разработки политики информационной безопасности организации (Политики).[1]

Важно, чтобы организация разработала Политику и чтобы она принимала в расчет цели организации и ее конкретные аспекты. Политика безопасности должна согласовываться с бизнесом организации, культурой, нормативной и правовой обстановкой, в которых действует предприятие. Разработка Политики необходима для целесообразности и

[1] В данном документе термин "Политика" является синонимом термина "политика информационной безопасности организации".

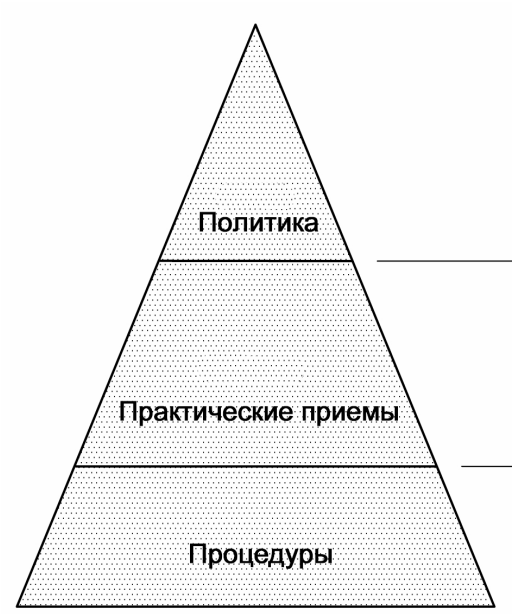
эффективности процесса менеджмента риска программы обеспечения. Для разработки и эффективного внедрения Политики нужна поддержка руководства во всей организации. Подстроив политику безопасности к бизнес-целями организации, Политика будет способствовать наиболее эффективному использованию ресурсов и обеспечит последовательный подход к обеспечению безопасности во всем спектре разных видов сред информационных систем.

## 5.4 Иерархия документации

### 5.4.1 Общий обзор

#### 5.4.1.1 Общая информация

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




Решение высшего руководства по обеспечению безопасности, описывающее общие принципы и цели безопасности.

Поддержка и дальнейшее разбиение общих принципов, обеспечивающие подробные меры, необходимые для выполнения требований политики по обеспечению безопасности.

Усовершенствование практических приемов на техническом уровне, обеспечивающее руководство по внедрению необходимых процедур.

Рисунок 1 - Документация программы

Документы, относящиеся к информационной безопасности, должны охватить как высокоуровневые цели организации, так и конкретные относящихся к безопасности настройки устройств, которые реализуют политику безопасности. Этот диапазон между общей и конкретной информации лучше всего представить несколькими уровнями документации. Число уровней должно быть сведено к минимуму, и данный стандарт рекомендует три уровня: документации - Политики, документация практических приемов обеспечения безопасности и документация операционных эксплуатационных процедур безопасности

По мере внедрения в организации новой прогрессивной технологии потребуются дополнительные документы. В то время, как документация Политики обычно будет пред-

[1] Номенклатура и иерархия не являются фиксированными. Организации могут использовать больше уровней иерархии и различную номенклатуру.

ставлена одной страницей, документация процедур может состоять из нескольких многостраничных документов, представляющих отдельные, специфические условия, организационные единицы и вопросы политики в организации. В некоторых случаях отдельная, вполне ограниченная система может также иметь собственную документацию практических приемов. Все практические приемы и процедуры должны перетекать с более высокого уровня к детальному уровню, поддерживая согласованность с оценками риска организации и общей Политикой.

#### 5.4.1.2 Политика информационной безопасности организации

Документ Политики является наименьшими по объему из всех документов в иерархии документов программы обеспечения информационной безопасности. Обычно Политика излагается в нескольких параграфах, 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, но она должна предоставлять конкретную информацию об активах, нуждающихся в защите, например, данные о клиентах, данные о сотрудниках, партнерские соглашения и процессы. Например, очень простая документация Политики может содержать единственное утверждение: "*Конфиденциальность, доступность и целостность всех информационных активов организации должны быть обеспечены посредством соответствующих защитных мер*".

Документация Политики – это абстрактная документация, всеобъемлющая по своему масштабу и наиболее важная из документов программы информационной безопасности по своему воздействию на организацию. Только единственный вариант документации Политики должен существовать в любой данный момент, и он должен быть распространен по всей организации. Он должен быть подписан членами правления, связанными с информационной безопасностью, например, главным исполнительным директором (CEO) и руководителем службы обеспечения информационной безопасности(CIO).

Документ Политики должен быть открытым по своему характеру, широко распространенным и доступным всем заинтересованным сторонам организации. В нем 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 получает свои полномочия непосредственно от должностных лиц организации и персонала на уровне правления. В документе должно быть заявление о намерении организации действовать в согласии с соответствующими местными и международными правовыми и нормативными структурами и основывать свою программу информационной безопасности на твердых принципах и практических приемов, признанных в национальных и международных стандартах по безопасности.

Документ Политики должен быть практически неизменным. Его изменение должно быть обусловлено изменениями стратегических целей, изменениями 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 управления изменениями.

#### 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 по финансам, физической безопасности и информационным технологиям.

#### 5.4.1.4 Классификация информации

Одним из аспектов реализации Политики является классификация информации. Во многом подобно "Совершенно секретным", "Секретным" и "Несекретным" военным системам финансовые организации имеют информацию различной ценности. Результаты классификации информационных активов будут показывать, когда следует внедрять хорошие, лучшие или наилучшие меры управления. Существует много типов системы классификации. Важным моментом для финансовой организации является определение классификационных уровней и использования классификации информации в вынесении решений о принятии риска. Например, риск, являющийся приемлемым для общественной информации, вероятно, будет неприемлемым для крайне секретной информации. Выгода классификации информации заключается в обеспечении поддержки руководству в отношении того, как служащие должны обращаться с информацией. Если документ, файл или база данных содержат информацию, относящуюся к различным классификационным 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 во время срока ее полезной службы. Эти изменения должны контролироваться согласно Политике организации.

### 5.4.2 Документы практики обеспечения безопасности

Документы практики обеспечения безопасности получены из содержания документации Политики. Эти документы определяют общие стандарты безопасности, которым должна следовать организация. Они отражают намерения и цели, установленные руководством самого высокого уровня при создании программы информационной безопасности, и документируют намерение реализовать политику независимым от технологии образом. Каждый документ практики обеспечения безопасности уже по своему масштабу значительно превышает документацию Политики. Каждый документ практики является технологически нейтральным и емкой формулировкой требований безопасности организации. Размер данного документа практики является переменным и зависящим от темы.

Число документов практики должно быть сведено к минимуму. Число необходимых документов различается в зависимости от величины организации и ее бизнес-потребностей, а также объема и сложности деятельности организации. Правовая и нормативная обстановка, оказывающая воздействие на организацию, может также влиять на число необходимых документов практики.

Документ практики не является общественным.[1] По своему характеру этот документ общего назначения является технологически нейтральным. Он менее абстрактный, чем документ Политики, и может оказывать меньшее влияние на всю организацию, поскольку применим только к некоторым аспектам организации. Например, очень простой документ практики может содержать простое утверждение:

"Аутентификация доступа к информационным активам организации должна осуществляться в соответствии с уровнем конфиденциальности активов. Аутентификация по двум факторам представляет собой минимально приемлемый уровень аутентификации; доступ к активам, классифицированным обладателем информации как "Конфиденциаль-

[1] Возможны обстоятельства представления документа практики регулятивным органам.

ные" должен осуществляться только посредством аутентификации по трем факторам.[1] Системы управления из двух факторов с доступом (основанные на биометрии и паролях) должны следовать следующим положениям..."

Хотя документы практики получают свои полномочия от Политики и должны строго соблюдать ее, они являются более изменчивыми, чем документы Политики. Это обусловлено тем, что они подвержены более частным изменениям, возникающим при идентификации новых рисков и мер управления безопасностью. Каждый документ практики имеет ограниченную аудиторию, так как он обычно затрагивает определенную часть организации или организационной единицы и не оказывает влияния на общую программу менеджмента безопасности организации.

Полезно включать в документацию обзорный раздел в котором указывается аудитория и владелец каждого документа практики. Владельцем практики может быть коммерческий директор, руководитель ИТ или руководитель группы технического сопровождения. Полезно также включать сведения о том, как классифицируется информация, связанная с данными практики, так как категория 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 различается в зависимости от темы и сложности процедур. Эти документы являются самыми сжатыми по своему объему из всех документов в иерархии документации. Они являются технологически конкретными выражениями того, как реализуется Политика. Документы применяются к реальным бизнес-системам, а определяемые поставщиком подробности о продукции приводятся в зависящей от платформы документации.

Документов операционных процедур должно быть столько, сколько необходимо, но при разработке документов необходимо проследить, чтобы они были полными, точными и целесообразными и чтобы ни один из них не противоречил любой другой практике или Политике. Примерные рекомендации, которые можно найти в очень простом документе процедур может содержать следующие инструкции:

"Используйте команду "pwadmin" для обеспечения соответствия паролей пользователей критериям, установленным в документации Практические приемы аутентификации и управления доступом организации. Дайте следующие команды..."

Документы процедур должны соответствовать общей Политике организации и практическим приемам, на которых основаны эти процедуры. Ни один документ процедур не должен противоречить основанной на политике практики 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, таких как внедренных мер управления на соответствие безопасности, список действий, которые нужно предпринять для мониторинга и анализа информационной безопасности при повседневном использовании, и отчеты об относящихся к безопасности инцидентах.

[1] Термин "аутентификация по трем факторам" 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 PINом или паролем. А для представления того, кем вы являетесь, используются биометрические данные.

# 6 Менеджмент информационной безопасности – Программа обеспечения безопасности

## 6.1 Общая информация

Для реализации Политики требуются программы обеспечения информационной безопасности. Этические ценности и управляющие распоряжения руководства организации должны распространятся и периодически подкрепляться руководством и персоналом на высшем уровне. Обеспечение информационной безопасности является коллективным процессом, а также индивидуальной обязанностью. Разработка, сохранение, улучшение и мониторинг программы обеспечения информационной безопасности требуют участия многих дисциплин организации. Необходима тесная координация между управляющими делами и персоналом обеспечения информационной безопасности. Для поддержки программы обеспечения информационной безопасности должны использоваться такие дисциплины, как аудит, страхование, нормативное соответствие, физическая безопасность, обучение, кадровая и правовая дисциплины и другие.

## 6.2 Создание программы

Наиболее важная рекомендация данного Технического Отчета состоит в том, чтобы организации создавали свою программу обеспечения информационной безопасности. Эта программа должна следовать из Политики, установленной для организации на высшем уровне руководства организации. 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 потребовать координация различных бизнес-функций организации, включая аудит, менеджмент риска, соответствие и страхование, служащих, отвечающих за нормативное и правовое соответствие, а также партнеров и клиентов.

## 6.3 Осведомленность

Программа улучшения осведомленности о безопасности должна включать функцию обучения и улучшения осведомленности о безопасности, гарантирующую, что все служащие остаются достаточно осведомленными и бдительными в отношении своих действий и действий окружающих их людей с последствиями для безопасности. Программа должна быть структурированной, для поддержания осведомленности служащих о своих связанных с безопасностью обязанностях и предоставлять ресурсы и поощрять тех, кто интересуется обеспечением безопасности, с целью расширения их знаний.

## 6.4 Анализ

Одному или нескольким должностным лицам организации должна быть установлена постоянная ответственность за программу обеспечения информационной безопасности. Установленные практические приемы 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 подробные процессы и процедуры, которые устанавливают учетность и ответственность за определение и отчет о надежности программы обеспечения информационной безопасности и ее соответствие требованиям.

Все отчеты анализа и мониторинга должны быть доступны руководству многих уровней, включая исполнительное руководство. Должны быть идентифицированы и документированы процедуры рассмотрения любых исключений из политики или отклонений от политики. Также должны существовать процедуры создания необходимых записей результатов аудита и записей о соответствии требованиям, а также мониторинга безопасности информации журналов регистрации. Особое внимание следует уделить идентификации рисков для информации журналов регистрации и требованиям, установленным для уменьшения этих рисков, гарантии адекватности защиты этих информационных активов.

### 6.5 Менеджмент инцидентов

Обо всех событиях информационной безопасности следует быстро сообщать, документировать и разрешать их в соответствии с практическими приемами организации. Когда нежелательные или неожиданные события информационной безопасности, имеют значительную вероятность компрометации бизнес-операций и создания угрозы для информационной безопасности, они становятся инцидентами информационной безопасности, которые подлежат рассмотрению как инциденты, так и события 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 официальные механизмы сообщения о вторжениях, неправильном срабатывании систем и других инцидентах безопасности, результаты расследования инцидентов безопасности, и 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 гарантировать, что практические приемы придерживаются установленной Политики и, что меры управления являются адекватными и эффективными. Все разрешенные отступления должны документироваться и ограничиваться во времени для проведения их периодических переоценок.

### 6.8 Поддержка

Все установленные защитные меры, такие как межсетевые экраны и программные средства обнаружения вирусов, должны регулярно обновляться, для поддержания их эффективности против новых возникающих угроз.

### 6.9 Восстановление после каких-либо бедствий

Программа обеспечения информационной безопасности должна определять информационные активы, являющиеся критичными для продолжения ведения бизнес- деятельности организации в случае ее прерывания. Программа должна создавать подробные письменные планы возобновления бизнеса после бедствий. Необходимо предусмотреть квалифицированный персонал, правовые соглашения, системы резервирования информации, ресурсы обработки и помещения для замещения тех, которые поддерживают

критическую бизнес-деятельность, и эти планы восстановления бизнеса после прерывания должны регулярно тестироваться и оцениваться.

# 7 Структура информационной безопасности

## 7.1 Приверженность

Приверженность в масштабе организации целям программы обеспечения информационной безопасности должна основываться на понимании как глобальных так и внутренних потребностей информационной безопасности организации. Организация должна демонстрировать приверженность программе посредством своей готовности выделять ресурсы для мероприятий, связанных с информационной безопасностью и рассматривать потребности информационной безопасности. На самом высоком уровне организации должна присутствовать осознание того, что значит информационная безопасность для организации, а также ее масштаб и объем деятельности.

Цели информационной безопасности необходимо распространить по всей организации. Каждый служащий или подрядчик должен знать свою роль и обязанности, а также свой вклад в обеспечение информационной безопасности и обладать полномочиям для достижения этих целей.

## 7.2 Структура организации

### 7.2.1 Роли и обязанности

Назначение программы обеспечения информационной безопасности заключается обеспечении конфиденциальности, целостности и доступности информационных активов. Достижение этих целей представляет собой междисциплинарную задачу. Соответствующее назначение и разграничение обязанностей должно быть связано с определенными ролями. Процедуры должны обеспечивать эффективное выполнение и осуществление всех важных задач.

### 7.2.2 Совет директоров

Совет директоров финансовых учреждений имеет обязанность перед организацией и ее членами по осуществлению надзора за практическими приемами менеджмента бизнес-деятельности организации. Эффективные практические приемы обеспечения информационной безопасности составляют разумную бизнес-практику и демонстрируют заботу о формировании общественного доверия. Совет директоров должен распространять идею о том, что информационная безопасность является важной целью, и поддерживать программу обеспечения информационной безопасности.

### 7.2.3 Комитет по аудиту

Комитет по аудиту в финансовой организации оказывает содействие совету директоров в осуществлении надзора и служит независимым подразделением для осуществления объективного анализа и баланса по внутренним мерам защиты и финансовой отчетности. Мониторинг и тестирование внутренних защитных мер, являющихся частью программы обеспечения информационной безопасности, входят в обязанности аудиторского комитета, обычно осуществляемых посредством функции внутреннего аудита организации и внешних аудиторов.

### 7.2.4 Комитет по менеджменту риска

Комитет по менеджменту риска, подчиняющийся совету директоров, должен пересматривать программу обеспечения безопасности и поддерживать финансирование про-

ектов, обеспечения информационной безопасности в том случае, когда эти проекты уменьшают операционный риск (и, следовательно, финансовый риск) организации. Комитет по менеджменту риска демонстрирует обязательство организации по обеспечению безопасности путем финансирования и поддержки проектов, выполняющих политики информационной безопасности организации. Комитет должен определять, какое воздействие на программу обеспечения информационной безопасности оказывают положения и законодательство, как это более подробно обсуждалось в пункте 5.2.

### 7.2.5 Правовая функция

Организации могут полагаться на специализированный опыт своего юридического отдела (или функции) в отношении некоторых аспектов менеджмента информационной безопасности. Юридическому отделу может быть вменено в обязанность осуществление мониторинга изменений законов посредством законодательства, положений и судебных дел, которые могут оказывать влияние на программу обеспечения информационной безопасности организации.

От юридического отдела может потребоваться проверка контрактов, касающихся служащих, клиентов, провайдеров услуг, подрядчиков и поставщиков для гарантии адекватного рассмотрения связанных с информационной безопасностью юридических проблем. Такие проверки могут включать 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 проявить желание основываться на экспортных заключениях при оценке последствий процедур урегулирования инцидентов безопасности и обеспечения их соответствия правовым требованиям среды функционирования, так как они различаются в соответствии с местной юрисдикцией. Юридический отдел должен быть вовлечен в разработку, поддержание и улучшение процедур управления действиями после инцидентов безопасности, такими, как сохранение свидетельств.

### 7.2.6 Исполнительные директоры

Главный исполнительный директор (CEO) или директор-распорядитель, как высшее руководство организации, несет конечную ответственность за ее функционирование. Главный исполнительный директор должен санкционировать создание программы обеспечения информационной безопасности, согласующейся с признанными стандартами оказывать ей поддержку, следить за выполнением важных решений, связанными с оценкой риска, и участвовать в пропаганде значимости обеспечения информационной безопасности.

В то время, как для многих организаций знакома должность главного исполнительного директора, финансового директора (CFO), руководителя технического отдела (CTO) и руководителя административной службы (COO), многие организации стали вводить такие дополнительные должности, как руководитель по информационным технологиям (CIO) и руководитель службы обеспечения информационной безопасности (CISO) на верхнем уровне структуры организации. Хотя существует много взаимозаменяемых функций руководителя технического отдела, руководителя по информационным технологиям и руководителя службы обеспечения информационной безопасности, каждая финансовая организация должна иметь руководителя службы обеспечения информационной безопасности, в конечном счете, учетного руководителю технического отдела или руководителю по информационным технологиям.

### 7.2.7 Управляющие делами

Управляющие делами, в частности и управляющие всей организации в целом, служат в качестве осуществляющих надзор и мониторинг агентов для организации и ее служащих. Эта делает их ключевыми участниками программ обеспечения информационной безопасности. Каждый управляющий должен понимать, оказывать поддержку и следовать Политике, практическим приемам и процедурам организации и обеспечивать подобное поведение служащих, поставщиков и подрядчиков. Управляющие делами должны создавать позитивную 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 их людей для безопасности. Служащие должны срочно сообщать обо всех подозрительных событиях, связанных с информационной безопасностью.

### 7.2.9 Не относящиеся к организации лица

Требования программы обеспечения безопасности должны быть включены в соглашения с подрядчиками и поставщиками услуг. Подрядчики и поставщики должны понимать, оказывать поддержку и следовать практическим приемам и процедурам обеспечения информационной безопасности организации и организационной единицы. Они должны соблюдать политику информационной безопасности организации. В то время как по экономическим или иным бизнес-причинам организации могут предпочесть привлечение внешних ресурсов для выполнения определенных банковских функций, менеджмент риска не может быть передан сторонним организациям и остается ответственностью организации.

### 7.2.10 Роли, связанные с безопасностью

#### 7.2.10.1 Введение

Здесь определяются три связанные с безопасностью роли в рамках программы обеспечения информационной безопасности. Эти роли наделяются разными уровнями обязанностей и функциями, необходимыми для выполнения программы обеспечения информационной безопасности. Эти роли являются функционально определенными, хотя способы обеспечения организацией административного управления персоналом, могут различаться.

В некоторых организациях отвечающий за информационную безопасность персонал может представлять собой отдельную административную единицу. В других организациях персоналу организационной единицы могут быть поручены связанные с информационной безопасностью обязанности в дополнение к собственным бизнес-обязанностям. Возможно также совмещение этих двух подходов.

Какую бы структуру не имела программа обеспечения информационной безопасности, исполнительные руководители и управляющие должны ей оказывать поддержку, чтобы сделать ее эффективной. В больших организациях может быть полезно разработать другие роли для эффективного выполнения специализированных функций, например, разработчик архитектуры безопасности. В более мелких организациях персоналу, вероятно, придется выполнять несколько ролей.

#### 7.2.10.2 Руководитель службы обеспечения информационной безопасности (CISO)

Руководитель службы обеспечения информационной безопасности отвечает за проектирование, внедрение и управление программой обеспечения информационной

безопасности. Под управлением руководителя службы обеспечения информационной безопасности персонал на других уровнях выполняет обязанности, осуществляющие политику и практические приемы программы обеспечения информационной безопасности. Руководитель службы обеспечения информационной безопасности может иметь специальный штат и осуществлять административное управление персоналом, отвечающим за информационную безопасность. По другому плану действий, руководитель службы обеспечения информационной безопасности может осуществлять ограниченный оперативный контроль за персоналом, выполняющим обязанности, связанные с информационной безопасностью, в дополнение к своим бизнес-обязанностям. Независимо от размера организации или стиля руководства, руководитель службы обеспечения информационной безопасности является лицом, несущим окончательную ответственность перед советом директоров и управляющими за выполнение программы обеспечения информационной безопасности.

Руководитель службы обеспечения информационной безопасности управляет выполнением программы обеспечения информационной безопасности в соответствии с условиями, определенными организацией как необходимыми 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 с бизнес-стратегией;

– руководство персоналом других уровней, который внедряет архитектуру безопасности и выполняет связанные с обеспечением информационной безопасности обязанности;

– проведение оценок риска, которые подтверждают правильность архитектуры безопасности и раскрывать недостатки, требующие внимания;

– публикацию политики, практических приемов и процедур обеспечения безопасности и управления программы повышения осведомленности о безопасности;

– осведомленность персонала о текущих угрозах и уязвимостях, а также новых методах и средствах обеспечения информационной безопасности для противодействия этим угрозам;

– обеспечение соответствующего вовлечения организации в усилия по защите критической инфраструктуры в странах, где организация ведет свой бизнес.

–

### 7.2.10.3 Ответственный за информационную безопасность (ISO)

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. Ответственные за информационную безопасность могут входить в штат руководителя службы обеспечения информационной безопасности или находиться под административным управлением организационной единицы организации. Ответственный за информационную безопасность может иметь особую должность, такую как разработчик архитектуры безопасности, имея обширные знания и опыт. Некоторые ответственные за информационную безопасность могут обладать специализированными знаниями в сфере методов и средств обеспечения информационной безопасности, таких как оценка риска, осведомленность об угрозах и т. д., и являться ресурсом для всей организации. Другие ответственные за информационную безопасность дают консультации и 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, опубликовывать их и обновлять по обстановке;

– 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 угроз информационной безопасности, технологий, а также методов и средств обеспечения информационной безопасности;

– способствовать осведомленности информационной безопасности.

#### 7.2.10.4 Операторы обеспечения безопасности

Операторы обеспечения безопасности выполняют наиболее детальные повседневные действия для осуществления целей программы обеспечения информационной безопасности. Операторы обеспечения безопасности могут быть в штате руководителя службы обеспечения информационной безопасности или относиться к другим организационным единицам организации. Они должны быть хорошо осведомлены об аппаратных и программных средствах и процедурах безопасности, необходимых для своих организационных единиц.

Из-за разнообразия технологий, которые могут использоваться в архитектуре безопасности, операторам обеспечения безопасности требуется выполнять множество процедур. Некоторые характерные обязанности, которые могут требоваться от операторов безопасности, включают: 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 для обнаружения связанных с безопасностью проблем. Широкое разнообразие задач показывает значимость операторов обеспечения безопасности для успешного функционирования программы обеспечения информационной безопасности.

Операторы обеспечения безопасности отвечают за:

– знание того, как роль оператора безопасности оказывает поддержку программе обеспечения безопасности и архитектуре безопасности;

– внедрение и поддержание практических приемов и процедур безопасности;

– мониторинг процедур безопасности и сообщение об их состоянии, по обстановке;

– работу над исправлением сбоев безопасности и противодействием атакам;

– восстановление соответствующих процедур безопасности во взаимодействии с восстановлением бизнеса после сбоя или атаки;

– предоставление рекомендаций по улучшению практических приемов и процедур.

# 8 Анализ и оценка риска

## 8.1 Процессы

Организации, которые желают получить доступ к состоянию дел со своей безопасностью, должны реализовать один или более процессов анализа риска как часть своей программы обеспечения информационной безопасности. Эти процессы должны использоваться для оценивания состояния безопасности всей организации, а также безопасности конкретных проектов, систем и продуктов. Поскольку стили руководства, размер и структура организаций различаются, могут потребоваться несколько стратегий для приспособления анализа риска к обстановке, в которой он используется.[1]

Результатом процесса оценки риска должны быть рекомендации по снижению рисков безопасности организации до приемлемого уровня. Эти рекомендации должны направлять выбор соответствующих защитных мер. Эти защитные меры являются результатом оценки и определения величины возможных потерь, которые могут произойти в случае, если идентифицированные уязвимости системы будут использованы одной или более угрозами. К активам организации, которые обычно подвергаются оценке риска, относятся: аппаратура и оборудование, прикладные программы, базы данных организации, системы связи и компьютерные операционные системы.

В Приложении D приводится пример метода проведения оценок риска и пример типичного процесса оценки риска. Дополнительные модели оценки риска можно найти в других документальных источниках, таких как ИСО/МЭК 13335 (все части) [4]. Примеры в Приложении D предоставлены с целью демонстрации и не должны использоваться непосредственным образом организацией в качестве технологических карт внедрения.

## 8.2 Процесс оценки риска

На финансовые учреждения и все другие предприятия оказывают влияние риски, относящиеся к их бизнесу. Риски, относящиеся к информационным активам предприятия, принимают многие формы и должны подвергаться методичному анализу. Оценки риска нужны для рассмотрения уязвимостей, угроз и рисков информации. Каждое банковское приложение обеспечивает контекст и знание рабочих процессов, а также потенциальных угроз и зон уязвимости. Это знание важно для проведения оценки риска. Оценка риска представляет собой трехступенчатый процесс:

1) оценка рисков потенциальных угроз для каждой зоны уязвимости путем заполнения табличной формы оценки риска (смотри пункт D.1);

2) присвоение комбинированного уровня риска каждой зоне уязвимости путем заполнения таблицы оценки риска (смотри пункт D.3);

3) определение подходящих политик безопасности и защитных мер, используя результаты шага 2 и имеющиеся меры управления.

Более подробный список категорий риска и их применения в процессе оценки риска представлен в Приложении C.

## 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,

[1] Дополнительную информацию можно найти в ИСО/МЭК 13335 (все части).

или для конкретных критических функций внутри системы. Не стоит ожидать, что оценка риска на уровне организации является просто комбинацией всех критических функций организации.

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

Тем не менее, любая оценка риска должна завершаться формированием набора рекомендаций по обеспечению оцененной системы. Эти рекомендации рассматривают риски, связанные с системой как риски, которые могут быть реализованы. В обязанность соответствующих управляющих делами входит принятие этих рисков. Во многих случаях можно применить дополнительные меры управления (или могли 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 случаев исключений из политики управляющий делами должен работать вместе с группой по обеспечению информационной безопасности гарантировать соответствие политике в будущем или чтобы долгосрочное исключение из политики было принято как остаточный риск.

# 9 Выбор и внедрение мер управления безопасностью

## 9.1 Уменьшение риска

Любая система обладает уязвимостями, посредством которых нарушители могут угрожать причинением финансовых потерь, потери продуктивности или утраты престижа организации. Минимизация и ослабление этих рисков является совместной обязанностью управляющих делами и группы по обеспечению информационной безопасности, работающих вместе с другими группами в финансовой организации. Существует много аспектов менеджмента риска, и многие наиболее значимые из них уже обсуждались: обязательство по обеспечению информационной безопасности высшего руководства, руководитель службы обеспечения информационной безопасности, отвечающий за внедрение и управление программой обеспечения безопасности, и сама программа обеспечения безопасности.

В пунктах 9.2 – 9.7 обсуждаются значимые процессы и технологии, обычно используемые или учитываемые для обеспечения ослабления риска. Они могут использоваться во время процесса разработки, после оценки слишком высокого риска или после идентификации новой уязвимости. Управляющие делами должны помнить о документированных преимуществах проектирования и встраивания безопасности в систему вместо попыток исправить существующую нарушенную систему.

Использование этих технологий может обеспечить непосредственное управление рисками, которые берет на себя организация. Организации нужно провести оценку того, как запланированные и существующие меры управления снижают риски, идентифицированные при анализе риска, определять дополнительные меры управления, которые имеются или могут быть разработаны, разработать архитектуру информационной безопасности и определить ограничения различных видов. Затем должны быть выбраны соответствующие и обоснованные меры управления для снижения оцененных рисков до приемлемого уровня остаточного риска. Дополнительные подробности, касающиеся выбора мер управления, можно найти в ИСО/МЭК 13335 [4] (все части).

## 9.2 Идентификация и анализ ограничений

На выбор мер управления могут оказывать влияние многие ограничения. Эти ограничения следует принимать в расчет при составлении рекомендаций и во время внедрения. Типичные ограничения и соображения включают следующее:

| Ограничения | Соображения |
|---|---|
| Временные | Меры управления должны быть внедрены за период времени, приемлемый для руководства, внедрены в течение срока службы системы и должны оставаться эффективными столько, сколько руководство считает необходимым. |
| Финансовые | Внедрение мер управления не должно быть более дорогостоящим, 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 приемлемости для персонала. |
| Связанные с окружающей средой | Выбранные меры управления должны быть приспособлены к доступности пространства, климатическим условиям, окружающей природной и городской географии. |
| Нормативные | Меры управления должны признавать правовые факторы, подобные защите персональных данных или не специфичным для ИТ законам из уголовного кодекса, и положения, типа инструкций пожарного отделения, трудового права и т. д. |

## 9.3 Логический контроль доступа

### 9.3.1 Общая информация

Логический контроль доступа относится к группе технических методов и мер управления, используемых 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 системные ограничения, ограничен проектирования или другие ограничения могут приводить к тому, что люди будут иметь некоторый дополнительный доступ. Тем не менее, необходимо наличие учетности доступа к системе: т. е. знание того, кому предоставляется право доступа, какие лица имеют доступ и когда этот доступ осуществлялся. Наиболее важной из всех является необходимость соблюдения определенных ограничений доступа. Для достижения эффективного контроля доступа должны быть введены следующие меры управления.

### 9.3.2 Идентификация пользователя

У многих различных видов пользователей может быть причина получения доступа к информации и информационным системам финансовой организации. Примерами этих видов пользователей 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 точную личность того, кто пытается получить доступ.

Традиционно каждая информационная система имела собственный процесс идентификации. При быстром расширении систем существует постоянная необходимость в процессе идентификации, который будет удовлетворять многим системам. Может оказаться возможным привлечение, внешних ресурсов для этих услуг по идентификации.

Приведенные ниже рекомендации должны применяться независимо от того, кто предоставляет услуги по идентификации.

Для обеспечения более высокой степени уверенности в личности пользователей организация должна создавать и осуществлять политики, требующие подтверждения личности пользователя перед выдачей идентификатора пользователя. Разумная бизнес-практика требует интегрирования требований "знай своего клиента" и "знай своих служащих" были интегрированы в мероприятия по выдаче идентификатора пользователя. Более того, организация должна создать процедуры и выполнять их для гарантии того, что до его выдачи каждый новый идентификатор пользователя является уникальным и может быть прослежен как до идентифицированного лица, так и лица, выдавшего идентификатор.

### 9.3.3 Санкционирование

Санкционирование является действием по предоставлению пользователю возможности выполнения определенных действий в системе на основе аутентификации личности пользователя. Организация должна определить права доступа каждого пользователя. Ни одному пользователю не должен быть разрешен доступ к какой-либо информации или приложению без специального санкционирования.

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

Другой принцип предназначен для распределенного сохранения записей со списком управления доступом по каждой системе или отдельным доступом для различных видов приложений (например, "тонкий" клиент, "толстый" клиент, сеть, многозвенное приложение, веб-сервисы 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 быть из внешних организаций, и неспособность аутентифицировать личность пользователя снижает возможность организации подтвердить учетность действий индивидуума и может сделать возможным несанкционированный доступ к данным и компьютерным ресурсам.

Существует несколько типов механизмов аутентификации. Их действие основывается на одной или нескольких следующих характеристик: что-то, что пользователь знает (например, пароли); нечто, известное пользователю (например, смарт-карта); какие-то физические характеристики пользователя (например, отпечатки пальцев или другие биометрические данные). Комбинирование разнообразных механизмов аутентификации может обеспечить более высокий уровень аутентификации.

#### 9.3.4.2 Цифровые сертификаты

Цифровые сертификаты могут использоваться для подписывания или шифрования информации и обеспечения аутентификации пользователя, кода программы или устройства. Цифровые подписи, основанные на сертификатах, могут использоваться для обес-

печения аутентификации источника информации, целостности данных и услуг неотказуемости. Основанные на сертификатах услуги по защите данных могут быть представлены с помощью шифрования. Стандарт ИСО 15782 определяет меры управления и синтаксис, необходимый для управления сертификатами X.509 в сфере финансовых услуг. Стандарт ИСО 21188 предоставляет подробную информацию о том, как осуществлять менеджмент информации о политике безопасности сертификатов в организации, и необходимые элементы формулировок практики, связанной с сертификатами.

#### 9.3.4.3 Пароли

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

Пароли могут быть либо динамическими (например, генерируемые и изменяемые автоматически и часто программными средствами), либо статическими (например, нечасто изменяемые по усмотрению пользователя). Рекомендации по формированию и контролю за использованием паролей можно найти во многих публикациях и в сети. "Рекомендации по управлению паролями Министерства обороны США" от 12 апреля 1985 года (CSC-STD-002-85) предоставляют техническую трактовку генерации, контроля и использования паролей в организации. Обсуждение на http://computing.fnal.gov/security/UserGuide/password.htm предоставляет более общую трактовку этой темы и включает дискуссию о составе и длине, изменении, хранении паролей и совместном использовании паролей.

#### 9.3.4.4 Биометрия

Биометрия является наукой идентификации людей по некоторым физическим характеристикам, которые могут быть измерены и с высокой степенью вероятности, являются уникальными для человека. Отпечатки пальцев – это, вероятно, самые известные биометрические данные. 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 узор сетчатки глаза, геометрию рук, черты лица и голос.

В стандарте ИСО 19092 [11] описывается, как можно осуществлять менеджмент биометрической информации в сфере финансовых услуг как часть программы менеджмента информационной безопасности организации. Данный Технический Отчет определяет цели контроля, меры управления и подробный журнал регистрации событий для осуществления менеджмента биометрической информации и достижения этих целей.

### 9.4 Журналы регистрации

Журналы регистрации представляют собой создаваемые системой записи осуществленной деятельности, используемые организацией как средство восстановления событий и введения учетности. Информация журнала регистрации необходима для разрешения проблем или споров, она так же предоставляет свидетельство для определения соответствия требованиям. Журналы регистрации помогают сдерживанию несанкционированной деятельности и обеспечивают раннее обнаружение подобной деятельности. Все системы должны обеспечивать некоторую степень подробности журнал регистрации в соответствии с политикой организации. Более того, уровень детальности должен быть как можно более подробным и согласовываться с практическими потребностями и поли-

тиками организации. По возможности, регистрация должна обеспечивать предупреждение ответственного лица в режиме реального времени о важных событиях, связанных с безопасностью.

Система регистрации должна оказывать поддержку быстрому расследованию и сообщать о подозрительной деятельности, чтобы содействовать сдерживанию и обнаружению несанкционированной деятельности. Анализ информации журнала регистрации руководством должен осуществляться регулярно, обычно ежедневно, и все исключительные и необычные ситуации, связанные с безопасностью, должны расследоваться и оформляться в виде отчета.

Информация журнала регистрации должна храниться в течение периода времени, соответствующего требованиям бизнеса. Эта 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 внедрить процедуры контроля за внесением изменений. Отсутствие этого контроля может привести к денежным потерям или падению продуктивности из-за ненадлежащей обработки или невыполненного обслуживания. Для изменений аппаратных средств, изменений программных средств как приложений, так и для управления патчами для операционных систем и процедур неавтоматизированных изменений должны существовать процедуры контроля таких изменений. Данные процедуры контроля за внесением изменений должны также учитывать управление такими изменениями в чрезвычайных ситуациях.

Управляющие делами должны обеспечивать надлежащие процессы контроля за внесением изменений для систем, находящихся под их управлением. Группа обеспечения информационной безопасности должна быть подготовленной, чтобы помогать осуществлять менеджмент связанных с безопасностью изменений и изменений систем безопасности, за менеджмент которых непосредственно отвечает группа информационной безопасности.

### 9.6 Осведомленность об информационной безопасности

Частью программы обеспечения информационной безопасности должна быть кампания по повышению осведомленности о безопасности с целью обучения служащих защитным мерам ценной информации организации. Программа предназначена оказывать позитивное влияние на отношение служащих к информационной безопасности. Повышение осведомленности о безопасности должно рассматриваться на постоянной основе.

Программа повышения осведомленности о безопасности должна предусматривать ознакомительный курс для новых служащих и служащих новой компании. Программа должна обучать пользователей в случае введения новых приложений или внесении значительных изменений в существующие приложения. Она должна постоянно рассматривать проблемы безопасности, появляющиеся в прессе.

Руководство и штат на различных уровнях имеют разные проблемы. При обращении к каждой группе должны быть выделены конкретные проблемы каждой группы. Презентации должны производиться таким образом, чтобы люди всех уровней и с различными навыками смогли их понять. Управляющие делами должны быть осведомлены о подверженности данных риску, рисках и потенциале потерь, а также нормативных требованиях и требованиях аудита. Это должно быть представлено как в условиях бизнес-деятельности, так и на примерах, относящихся к сфере ответственности управляющего делами, где наиболее эффективными являются позитивные сообщения.

### 9.7 Человеческие факторы

Рабочая сила представляет собой один из наиболее важных активов финансовой организации. Заинтересованность и сотрудничество служащих очень важны для успешной реализации программы обеспечения информационной безопасности. Благодаря возросшей осведомленности о безопасности служащие будут внимательны и станут замечать отклонения от нормы в технологии или операционных процедурах организации, которые могут указывать на возможную проблему безопасности.

С другой стороны, люди также делают ошибки. Они могут неправильно использовать технологию. Они могут также совершать преступления. Эти человеческие недостатки делают необходимыми переговоры руководителя службы обеспечения информационной безопасности со всеми отделами организации при разработке программы обеспечения информационной безопасности и повышения осведомленности служащих. Другие отделы могут вносить свой вклад в виде представления мнения о служащих организации, чтобы минимизировать вероятность ошибок и криминальной деятельности.

Определенные должности в организации могут быть определены как "доверенные", потому что эти должности разрешают доступ или требуют доступа к конфиденциальной кадровой или финансовой информации. Другую доверенную должность занимает служащий, имеющий широкие привилегии или возможности, связанные с компьютерами или активами ИТ организации. Персонал, выбираемый на "доверенные" должности, должен отличаться высокой честностью и проходить проверку биографических данных. Служащим, занимающим доверенные должности, следует дать совет о необходимости ограничения обсуждений с семьей и знакомыми конфиденциальных бизнес-процедур. Бизнес-конкуренты могут пытаться прибегнуть к социотехнике, подстрекательству человека раскрыть информацию несанкционированным лицам. Подстрекатель использует ложный интерес к работе человека, технические дискуссии и лесть, чтобы побудить служащего нечаянно раскрыть конфиденциальную информацию.

## 10 Меры управления системами ИТ

### 10.1 Обеспечение защиты систем ИТ

Существует много способов обеспечения защиты систем ИТ. Данные меры управления могут включать в себя политики организации. Однако для целей данного пункта 10 меры управления будут представлены настройками системы и внешними контрмерами (подобно шифрованию), которые могут использоваться для обеспечения аутентификации, санкционирования, конфиденциальности, целостности, доступности и других услуг безопасности. Будут обсуждаться контрмеры и меры управления, которые применяются в настоящее время, и будут применяться в будущем.

В дополнение к первоначальному размещению мер управления и контрмер организация должна предпринять шаги для обеспечения их долгосрочного функционирования и поддержки. Иначе с течением времени, когда станут известны новые уязвимости, а выпущенные патчи будут игнорироваться, безопасность системы ослабнет. Хорошо действующая программа обеспечения безопасности включает процессы и процедуры поддержки, которые обеспечивают наличие необходимых мер управления и их постоянное обновление.

### 10.2 Защитные меры аппаратных систем

Обеспечение защиты аппаратных систем в среде ИТ является решающим для целостности информационных активов. Некоторые из наиболее важных мер управления

для защиты критических ресурсов обсуждаются в Приложении D. В данном Техническом Отчете не делается попытка включить в него всеобъемлющий список всех ресурсов ИТ, которые может использовать организация, а скорее включается краткое обсуждение каждого из нескольких главных типов ресурсов, и некоторые соответствующие меры управления, которые могут использоваться для предотвращения угроз этим ресурсам, представлены в пункте D.1. Каждое обсуждение происходит по одной схеме. В каждом обсуждении рассматриваются ключевые вопросы. Они включают рассмотрение того, почему та или иная система является важной, какие зоны безопасности могут быть наиболее важными и какие меры управления должны быть рассмотрены.

Одним из вопросов, которому не уделяется внимание и, который организации иногда не учитывают,, являются поставщики аппаратных систем. Обычно принимается на веру, что производители и поставщики оборудования действуют от имени финансовой организации и достаточно осведомлены о целях и политиках безопасности. Однако есть вероятность, что машины, поставляемые производителем или торговым посредником, могут быть сконфигурированы на предоставление несанкционированного доступа к информации или сетевым соединениям. Произвольное приобретение и случайное распределение машин в сети могут содействовать защите от этого вида преднамеренной или непреднамеренной угрозы безопасности. Для приложений с высокой степенью безопасности, может быть, следует рассмотреть меры управления, создающие доверие между организацией и поставщиком.

Оценивание аппаратных средств, такое как в соответствии с FIPS 140-2[1] [17] должно считаться необходимым, в особенности, для криптографических устройств. Для других устройств при выборе и использовании устройства следует полагаться на оценки по соответствующим общепринятым критериям или специализированным профилям защиты.

### 10.3 Безопасность программного обеспечения.

Поскольку современные финансовые учреждения полагаются на автоматизацию при обработке практически всех своих бизнес-операций, в основе программы обеспечения информационной безопасности лежит безопасность программных систем. Обеспечение безопасности ПО затруднено в следствие его сложности, множества взаимодействий и разнообразных способов доступа к программным средствам. Кроме того, многие системы, подобные межсетевым экранам, веб-серверам и серверам приложений, предназначены для работы на многих аппаратных платформах. В материале, приведенном в пункте A.2, рассматривается безопасность систем программного обеспечения на высоком уровне, так как существует обширная литература, в которой подробно обсуждается вопрос обеспечения безопасности каждого типа систем программного обеспечения.

### 10.4 Меры управления сетями и сетевыми системами

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

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

Сетевой трафик уязвим перед атаками, связанными с изменением маршрутизации, копированием и сетевым анализом пакетов[1], которые легко могут пройти полностью необнаруженными сетью и системами, использующими сеть. Хотя шифрование часто рассматривается как главное решение обеспечения безопасности, шифрование сетевого уровня может быть слишком дорогостоящим, с точки зрения осуществления, пропускной способности и создаваемой задержки для многих предприятий. Даже при использовании протоколов SSL, IPSEC и других протоколов безопасности связи, они не обязательно являются первым этапом защиты для сетевой безопасности. Для осуществления управления защитой сети следует обратить внимание на положения стандарта ИСО/МЭК 18028.

Вместо этого первым этапом защиты часто является договорное соглашение между организацией и провайдером телекоммуникационных услуг, а также доверие к провайдеру телекоммуникационных услуг. Поэтому использование известных провайдеров телекоммуникационных услуг, с четко определенными соглашениями об уровне сервиса и точным языком контракта, часто является первой и наиболее важной мерой управления. Следующей наиболее важной мерой управления сети будет система граничных мер управления (как описано в пункте 10.5), используемых для обеспечения безопасности, мониторинга и управления соединениями между внутренними и внешними сетями организации.

## 10.5 Граничные меры управления и меры управления взаимодействия

### 10.5.1 Общая информация

В литературе много написано о все увеличивающейся открытости корпоративных сетей. То, что когда-то было прочным, жестко контролируемым периметром, стало открыто для веб-сервисов, бизнес-сотрудничества, поддержки сторонними организациями, взаимодействия клиентов с системами регистрации, временных работников и работников по договору, а также доступа служащих – как удаленного доступа из дома, так и внешних соединений с другими фирмами. Все увеличивающаяся проницаемость границы организации означает, что граница и системы взаимодействия продолжают являться критическим элементом информационной безопасности организации. Проницаемость также означает, что все больше и больше устройств являются возможными точками проникновения для злоумышленной деятельности. Для этих устройств необходимо рассмотреть возможность применения межсетевых экранов, систем обнаружения вторжения и, возможно, других мер управления, как отмечалось в описании конечных систем в пункте D.1.

Все эти граничные связи между предприятием и большой средой с сетевой структурой являются критичными; любая граница представляет возможность для угроз совершить атаку, используя уязвимости систем предприятия. Предприятия должны определить собственные политики, касающиеся того, как должны применяться граничные меры управления. К примеру, организация может потребовать изолирования для создания безопасной среды с высокой степенью защиты, например, где все пользователи и конечные системы будут физически соединены внутри здания организации. С другой стороны, организация может обеспечивать защиту всех своих активов в защищенной базе данных за безопасным сервером веб-приложений, за многими уровнями межсетевых экранов и программных средств обнаружения вторжения или со строгой аутентификационной проверкой пользователей. Что из этого является приемлемым, зависит от активов организации, оценки риска и принятых политик.

[1] «Анализатор пакетов» – это программа, анализирующая информационные пакеты, во время их перемещения по сети, осуществляя поиск информации, которая может использоваться для совершения атаки, как например, содержание сообщений электронной почты, имена и пароли пользователей или сетевые адреса.

### 10.5.2 Межсетевые экраны

Межсетевые экраны представляют собой развитую технологию для обеспечения граничных мер управления на сетевом уровне. В то время как существуют вариации 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 предприятия. 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 будет открыт только для очень небольшого набора 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 или DMZ. Веб-серверы и другие направленные вовне серверы и сервисы размещаются 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 для управления 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.

Исторически, межсетевые экраны были программными средствами специального назначения или специальными устройствами, размещающимися на сетевом тракте и защищающими крупные участки предприятия; они были важным элементом прочности укрепленных периметров. В последние 2-3 года межсетевые экраны были внедрены в конечные системы, часто в качестве так называемых персональных межсетевых экранов. Обе тенденции – межсетевые экраны вида специальных устройств для важных сетевых соединений и персональные межсетевые экраны на персональных компьютерах и других конечных системах – продолжают развиваться.

Новейшей тенденцией является комбинация функциональных возможностей межсетевых экранов с возможностью обнаружения вторжений.

### 10.5.3 Система обнаружения вторжений (IDS)

Межсетевые экраны часто принимают или отвергают соединения на основе адреса, порта и протокола. В пределах этих параметров может быть много возможных потоков данных, фактически являющихся атаками или вредоносным программным обеспечением, а также множество законных потоков данных, предназначенных для поддержки законной бизнес-деятельности. Системы обнаружения вторжений рассматривают данные в пакетах и сравнивают их с характеристиками известных атак. Затем системы обнаружения вторжений посылают предупреждения электронным почтовым сообщением, телефонным звонком или на пейджер соответствующему персоналу организации. Существуют два основных вида систем обнаружения вторжения: сетевые детекторы, подключенные к сетевым маршрутизаторам, коммутаторам и серверам и рассматривающие трафик в сети; детекторы на базе хоста, представляющие собой программное обеспечение, загруженное

на серверы и конечные системы, которое рассматривает трафик, связанный с определенным устройством. Оба типа детекторов все шире используются на предприятиях.[1]

Одним из главных недостатков систем обнаружения вторжения является зависимость от известных характеристик атак, тогда как новые атаки с неизвестными характеристиками могут проскользнуть незамеченными. Системы обнаружения вторжения начали с поиска отклонений в поведении таких систем, как ftp трафик, где обычно присутствует только http трафик, или трафик 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 производить анализ поиска отклонений не только на границах, но также в самой сети предприятия.

Некоторые аналитические средства являются чисто средствами, зависящими от других устройств для сбора данных, используемых для поиска отклонений. Межсетевые экраны и системы обнаружения вторжений начинают объединяться; часто поставщик предлагает комбинированные изделия, выполняющие функции и межсетевого экрана, и системы обнаружения вторжений. Эти комбинированные изделия также используются в настоящее время – особенно когда 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 совершенно приемлемая практика, существует компромисс, так как другой законный трафик может проходить через то же соединение. Организации должны для себя определить, когда цена разрешения законного трафика перевешивает возможный ущерб от атаки.

Эта субъективная оценка в отношении допущения возможных атак в сопоставлении с вероятным ущербом от атаки, выявляет один из недостатков систем обнаружения вторжений. Практически в любой системе обнаружения вторжений будет некоторое число ошибочных результатов. Т. е. в некоторых случаях система обнаружения вторжений выдает предупреждение о трафике, выглядящего как атака, но в действительности являющегося законным. Аналогичным образом существует (очень незначительная) вероятность того, что атака останется необнаруженной. Системы обнаружения вторжений обеспечивают организациям значительную гибкость в настройке системы, чтобы минимизировать ошибочные результаты и ошибочные реагирования на атаки.

### 10.5.4 Другие защитные контрмеры

Существует много других защитных мер для сетевых границ и связности. Различные случаи использования требуют разных подходов. Например, близкий бизнес-партнер может иметь прямое соединение с внутренней сетью или маршрут может быть проложен через единственный межсетевой экран, а не через два межсетевых экрана. Маршрутизаторы и коммутаторы, составляющие внутренние сети организации, должны быть надежно защищенными и хорошо управляемыми. Многие функции межсетевого экрана действуют как защитный слой за функциями маршрутизации, уже выполненными сетевой инфраструктурой. Вне сети, межсетевых экранов и систем обнаружения вторжения существуют две другие основные контрмеры: шифрование и аутентификация. Очевидно, что шифрование, может использоваться для защиты частной информации. Ее можно выполнить на многих уровнях и во многих местах, но за определенную цену. Эти компромиссы должны быть оценены относительно политики организации и ценности информации организации.

[1] Отметьте, что в группе Методов и средств обеспечения безопасности ИТ JTC 1/SC 27 начата работа по определению стандарта IDS, ИСО/МЭК 18043.

Аутентификация может использоваться для идентификации устройств, а также пользователей устройств (включая "пользователей" программного обеспечения). Устройства можно идентифицировать, используя IPSEC, или в некоторой степени посредством протокола безопасности SSL. Конечный пользователь может быть аутентифицирован через SSL, хотя SSL не может реально аутентифицировать фактического пользователя – физического лица (некоторые браузеры, например, запоминают имена пользователей и пароли, так что любой, использующий этот компьютер и браузер, будет казаться Джоном Смитом с точки зрения веб-сервера). Использование различных факторов, а не только идентификатора пользователя и пароля, может улучшить качество аутентификации, но это может сделать и обладание маркером или смарт-картой, обладание секретным ключом, связанным с цифровым сертификатом, или отпечатки пальцев (или другие биометрические характеристики).

# 11 Внедрение специальных средств защиты

## 11.1 Банковские карточки для финансовых операций

### 11.1.1 Общая информация

Банковские карточки для финансовых операций могут быть карточками с магнитной полосой, которые могут хранить информацию на магнитном носителе, или "смарт-картами"[1], которые могут обрабатывать информацию, выполнять криптографические функции и хранить гораздо больше информации, чем позволяет магнитный носитель. Поскольку смарт-карты обладают большей гибкостью, чем карточки с магнитной полосой, в будущем может быть разработано и другое использование этих карт. По вопросам безопасности смарт-карт обращайтесь, пожалуйста, к стандарту ИСО 10202.

Ассоциации 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 управления.

### 11.1.2 Физическая безопасность

Для обеспечения 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 мощностью собственных нужд.

### 11.1.3 Злоупотребление со стороны инсайдеров

Для предупреждения мошеннических операций, осуществленных в результате доступа к информации на банковских карточках, все носители, содержащие действительную информацию о счетах, номера счетов, личные идентификационные номера, кредитные лимиты и состояние счетов, должны храниться в помещении, доступ к которому ограничивается выбранным персоналом. Функции изготовления и выпуска карточек должны

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

быть физически отделены от функций создания 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 со стандартом ИСО 9564-1 – 4 или ИСО 10202-1 – 8. ИСО 9564 определяет основные принципы и методы обеспечения мер минимальной безопасности, необходимых для эффективного международного менеджмента личных идентификационных номеров. Он также определяет методы защиты личных идентификационных номеров, применимые для операций с применением банковских карточек для финансовых операций в условиях режима реального времени, и стандартные средства обмена данными личных идентификационных номеров. Стандарт ИСО 9564 также распространяется на менеджмент и безопасность личных идентификационных номеров в условиях режима реального времени и условиях электронной торговли. Эти методы и средства должны использоваться организациями, отвечающими за внедрение методов менеджмента и защиты информации личных идентификационных номеров в банкоматах (ATM) и финансируемых покупателями кассовых терминалах (POS).

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

Данный Технический Отчет не распространяется на неприкосновенность данных операций, 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 информации личных идентификационных номеров в банкоматах (ATM) и финансируемых покупателями кассовых терминалах (POS). ИСО 10202 определяет принципы защиты интегральных микросхем в течение их жизненного цикла, от производства и выпуска, использования клиентами и служащими до прекращения действия. В 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 ИСО 10202. В нем также описываются требования безопасности для модулей приложений, которые могут быть добавлены к устройству считывания карточек.

### 11.1.5 Персонал

Для предупреждения поручения неподходящему персоналу обязанностей по обработке кредитных карточек должны проводиться кредитные проверки и проверки судимостей для всех служащих, имеющих дело с проштампованными или неиндоссированными карточками, включая служащих, занятых неполный рабочий день, и временных работников, где это разрешено законом.

### 11.1.6 Аудит

Для обеспечения целостности управляющей информации и регистрационной информации требуется, чтобы меры управления и журналы регистрации поддерживались

для пластиковых листов с отпечатанными данными, печатных форм, штамповочного и шифрующего оборудования, защитной фольги, голограмм, магнитной ленты, полуфабрикатов карточек и готовых карточек, карточек образцов, информации о номерах счетов владельцев карточек и оборудования для устранения отходов.

### 11.1.7 Предупреждение подделки карточек

Для предупреждения использования информации, раскрытой на товарных чеках, для создания фальшивых карточек с магнитной полосой, на магнитной полосе должны быть зашифрованы цифры криптографической проверки, и эти цифры должны подтверждаться как можно большим числом операций.

Для предупреждения использования перехваченной информации для создания фальшивых карточек необходимо использовать в идентификации физический метод карточки (CAM) для подтверждения подлинности карточек.

### 11.1.8 Банкоматы

Банкоматы (ATM) представляют собой устройства, позволяющие клиенту проверить остаток на счете, изъять и положить наличные, оплатить счета или осуществить другие функции, которые обычно ассоциируются с банковскими кассирами. Эти устройства могут находиться внутри зданий организации, размещаться за пределами такого здания или находиться вдалеке от помещений организации.

Рекомендуются дополнительные меры предосторожности для снижения возможности ограбления клиентов и вандализма в отношении машин, но они находятся за рамками данного Технического Отчета. Производители таких устройств и поставщики сети банкоматов обычно публикуют руководства по безопасности пользования банкоматами. Следует принимать во внимание эти документы. Операции, осуществляемые банкоматами, должны соблюдать требования безопасности, которые определены в системах оплаты по карточкам.

### 11.1.9 Идентификация и аутентификация владельцев карточек

Наиболее распространенным средством аутентификации владельца карточки является личный идентификационный номер (PIN). Он используется для управления доступом к банкоматам и кассовым терминалам. Пользователи должны знать, что обеспечение секретности личного идентификационного номера является их обязанностью. В дополнение к личному идентификационному номеру для идентификации владельцев карточек начинают находить применение биометрические данные и другие технологии.

Для предотвращения несанкционированных операций, вызванных отгадыванием личного идентификационного номера карточки, используемых несанкционированным лицом, число попыток ввода личного идентификационного номера должно быть ограничено тремя. После трех неудачных попыток рекомендовано задержание карточки и установление контакта с ее владельцем.

### 11.1.10 Аутентичность информации

Для предотвращения несанкционированного изменения информации, передаваемой в банкомат и из него, для каждой передачи следует требовать использования кода аутентификации сообщений (MAC), созданного в соответствии с требованиями ИСО 16609 и распространяемого в соответствии с требованиями 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 ИСО 9564. Следует рассмотреть возможность шифрования всей информации, передаваемой из банкомата. Управление личными идентификационными номерами должно осуществляться в соответствии с необходимыми стандартами ИСО.

#### 11.1.12 Предотвращение мошенничества

Для обнаружения и предотвращения мошеннического использования банкоматов, такого как подделка чеков, депозиты пустых конвертов или дезавуированные операции, рекомендуется целый ряд практических приемов. Они включают в себя ограничение числа операций и суммы денежных средств, снимаемых в день с одного счета, ежедневное подведение баланса банкомата под двойным контролем, установку видеокамер, где опыт мошенничества или его возможность оправдывают это, и поддержку работы банкомата в онлайновом режиме, где это возможно, т.е. требование, чтобы банкомат имел возможность проверки состояния счета до совершения операции. Если работа в режиме реального времени невозможна, следует установить более строгие требования к выпуску карточек, чем в случае работы в режиме реального времени.

#### 11.1.13 Техническое обслуживание и текущий ремонт

Для предотвращения несанкционированного доступа к информации во время технического обслуживания и технического ремонта банкоматов следует убедится, что банкоматы находятся в состоянии "не работает" для клиентов перед проведением любого технического обслуживания. Для текущего ремонта банкоматов, включающего открытие 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 (EFT), могут оцениваться независимо от технологии, которую они используют. Для предотвращения потерь из-за принятия запроса о платежах от несанкционированного источника должна производиться аутентификация источника сообщений с запросом о переводе платежей. Аутентификация источника должна быть основана на процедуре безопасности, определенной в договоре с клиентом или лицом, с которым ведется переписка. Там, где стоимость и выполнение криптографической аутентификации делают ее выполнимой, рекомендуется применение этого средства контроля.

Код аутентичности сообщений (MAC), генерируемый в соответствии с требованиями
ИСО 16609, с криптографическим ключом, распределенным в соответствии с требованиями
ИСО 11568, обеспечивает криптографическую аутентичность. Альтернативным образом для установления подлинности источника сообщения может быть использовано успешное дешифрование сообщения, зашифрованного с соответствии с ИСО/МЭК 18033 (в соединении с ИСО/TR 19038 [10] или ANSI X9.52 [14]) или FIPS 197 [18], с ключом, распространяемым в соответствии с 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, валюту, имя бенефициара и, возможно, номер счета бенефициара или IBAN компоненты сообщения, используя процедуру безопасности, определенную в договоре с клиентом или лицом, с которым ведется переписка. Там, где это осуществимо, следует использовать полную аутентификацию текста. Рекомендуется применение криптографической аутентификации.

### 11.2.3 Воспроизведение сообщений

Для предотвращения несанкционированного повторного платежа, вызванного воспроизведением сообщения, требуйте использование и верификацию однозначной идентификации сообщения. Включайте эту идентификацию в любую проводимую аутентификацию.

### 11.2.4 Сохранение записей

Для сохранения свидетельств, которые могут потребоваться для доказательства санкционирования при совершении платежа, регистрируйте сообщения с запросом о переводе платежей независимо от носителя, используемого для передачи сообщений. Надо сохранять материал, необходимый для подтверждения аутентификации, включая вспомогательный криптографический материал.

### 11.2.5 Правовая основа для платежей

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

## 11.3 Банковские чеки

### 11.3.1 Общая информация

Банковские чеки, также известные как платежные приказы и использованием средств сберегательного счета клиента в банке, представляют собой письменные распоряжения, предписывающие финансовой организации выплатить деньги. Некоторые новые подходы к обработке чеков должны повысить значимость проблем безопасности для финансовых учреждений. Престиж банковского чека и других компонентов сокращения процедуры обработки документов является примером методов, повышающих значимость безопасности. Многие национальные организации опубликовали стандарты по различным аспектам операций обработки чеков[1].

### 11.3.2 Новые клиенты

Требование "знай своего клиента" создает особенные проблемы, когда услуги предоставляются через открытую сеть. В то время как может показаться желательным рекламировать услуги, использующие базовую веб-страницу или другой электронный носитель, личное посещение офиса финансовой организации остается необходимым условием для открытия нового счета (за исключением действия в соответствии с юридически установленным методом), пока не будет доступен повсеместно признанный и имеющий ис-

[1] Подкомитет В X9 (США) опубликовал стандарты по операциям обработки чеков, такие как ANSI X9 TG-2 *Понимание и разработка чеков* и ANSI X9 TG-8 *Принципы безопасности чеков.* Для достижения согласованного действия финансовых организаций и улучшения качества обработки финансовым организациям настоятельно рекомендуется следовать указаниям Технического руководства 2 (TG-2) X9 и Технического руководства 8 (TG-8) X9.

ковую силу электронный метод позитивной личной идентификации. Следует соблюдать обычные процедуры оценки квалификации клиентов.

#### 11.3.3 Вопросы целостности

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

Запросы на финансовую операцию должны быть снабжены цифровой подписью, используя ключ, подтвержденной органом сертификации организации. При надлежащей реализации это должно обеспечить уверенность в том, 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 раскрытия сделают возможным несанкционированное использование счета, должны быть защищены с помощью шифрования.

# 12 Разное

## 12.1 Страхование

Планируя программу обеспечения информационной безопасности, работник службы информационной безопасности и управляющий делами должны консультироваться со страховым отделом и, если это возможно, со страховой компанией. В результате это должно привести к более эффективной программе 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 имеют дело с мерами управления информационной безопасности. Поскольку эти меры управления должны присутствовать для страховых целей, они должны быть включены в программу обеспечения информационной безопасности организации. Может также требоваться гарантирование некоторых мер управления, т. е. могло показать, что они постоянно присутствовали с момента принятия политики.

Страховая компенсация прерываний бизнеса и в особенности ошибок и упущений должно быть включено в планирование обеспечения информационной безопасности.

## 12.2 Аудит

Приведенная ниже цитата из заявления Института внутренних аудиторов определяет роль аудитора следующим образом:

"Внутренний аудит является независимым и объективным мероприятиям консультирования и обеспечения доверия, предназначенным для добавления ценности операциям организации и их совершенствования. Он помогает организации в достижении ее целей путем введения систематического и упорядоченного подхода к оцениванию и повышению эффективности процессов менеджмента риска, контроля и управления. Внутренний аудит проверяет надежность и целостность информации, соответствие политикам и положениям, защиту активов, экономное и эффективное использование ресурсов и действующие оперативные задачи и цели".

Говоря более конкретно, в сфере информационной безопасности аудиторы должны оценивать и тестировать защитные меры в отношении информационных активов финан-

совой организации и вести постоянный диалог с работниками службы информационной безопасности и другими лицами для выработки соответствующих перспектив для идентификации угроз и рисков, а также адекватности защитных мер для существующей и новой продуктции.

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

### 12.3 Планирование восстановления после бедствия

Важной частью программы обеспечения информационной безопасности является план по продолжению критической бизнес-деятельности в случае прерывания. Восстановление после бедствия является частью планирования возобновления бизнеса, которое гарантирует, что информация и средства обработки информации будут восстановлены как можно быстрее. План восстановления после бедствия идентифицирует диапазон бедствий, против которых должна обеспечиваться защита, и определяет функции и обязанности персонала в таких условиях.

План восстановления после бедствия должен включать точный список тех действий бизнеса, которые считаются критичными, предпочтительно с категориями приоритета, а также интервалы времени восстановления, являющиеся адекватными для выполнения бизнес-обязательств организации. План должен определять связанные с ресурсами обработки помещения, имеющиеся для замены тех, которые поддерживают критическую бизнес- деятельность.

В случае если персонал не способен доложить организации о содействии восстановлению после бедствия, необходимо определить замещающий персонал, способный восстановить и эксплуатировать ресурсы обработки информации. Если это возможно, организация должна стремиться к заключению соглашений с поставщиками услуг о приоритетном восстановлении услуг. План восстановления после бедствия должен обеспечивать доступность адекватных дублирующих информационных систем, способных своевременным образом обнаруживать и извлекать критическую информацию.

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

План восстановления после бедствия должен тестироваться так часто, как это необходимо для обнаружения проблем и продолжения обучения персонала в процессе его деятельности. Должна проводиться периодическая переоценка плана восстановления после бедствия, чтобы убедиться, что он по-прежнему уместен для своих целей. Организация должна определить минимальную частоту проведения как тестирования, так и переоценки.

### 12.4 Внешние поставщики услуг

Финансовые учреждения требуют, чтобы к предоставляемым из вне критическим услугам, таким как обработка данных, обработка финансовых операций, сетевые услуги и создание программного обеспечения, применялись защитные меры и защита информации такого же уровня, как такая же деятельность, проводимая в самой организации. Кон-

тракты с внешними поставщиками услуг должны включать элементы, необходимые, чтобы убедить финансовую организацию 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 выше сказанному, специалистами финансовой организации должна быть проведена независимая финансовая проверка поставщика услуг до заключения контракта с поставщиком услуг.

Никакие дела с поставщиком услуг не должны вестись, пока не будет получено гарантийное письмо, подтверждающее наличие защитных мер информационной безопасности. Руководитель службы обеспечения информационной безопасности должен проверить программу обеспечения безопасности поставщика услуг, чтобы определить, согласуется ли она с программой организации. Любые недостатки должны разрешаться либо путем обсуждения условий с поставщиком услуг, либо посредством процесса принятия риска в организации.

В дополнении к требованиям информационной безопасности договоры с поставщиками услуг должны включать требования о неразглашении и четкое определение ответственности за потери, вытекающие из упущений в обеспечении информационной безопасности.

### 12.5 Группы тестирования на проникновение

Использование специалиста по тестированию на проникновение, обычно подрядчика, для оценки эффективности безопасности системы посредством попытки проникновения в систему с ведома и при согласии соответствующего должностного лица организации, является одним из методов достижения доверия к программе обеспечения безопасности.

По мере усложнения компьютерных систем, поддерживать безопасность становится все труднее. Использование групп тестирования на проникновение может помочь в нахождении определенных слабых мест системы организации. Однако необходимо принимать во внимание некоторые вопросы. Подрядчик должен быть связан соответствующими обязательствами или обладать достаточной стабильностью, чтобы удовлетворять любым обязательствам, вытекающим из его действий.

Организация не должна полагаться только на отчеты тестирования на проникновение для контролирования своей программы обеспечения безопасности.

Неразглашение результатов должно быть указано в контракте со специалистами по тестированию на проникновение. Любое раскрытие проблемы безопасности должно происходить по усмотрению организации.

### 12.6 Криптографические операции

Развитие ИТ сделало традиционные методы контроля информации значительно более сложной задачей. Популяризация криптографических устройств предоставила финансовым учреждениям возможность повторно достичь уровня безопасности, ранее свя-

занного с банковским делом, пожиная при этом плоды развившейся технологии обработки информации.

Как и в случае с любой новой технологией, существует опасность неправильного использования криптографических решений. Важно, чтобы организации принимали соответствующие решения о выборе, использовании и постоянном оценивании своих защитных мер, основанных на применении криптографии.

Предполагается, что потребность в криптографических защитных мерах определена. Защитные меры, предлагаемые в пунктах 9 – 15, используют шифрование, коды аутентификации сообщений и цифровую подпись. Для каждой из этих услуг также требуется распределение ключей или услуги по сертификации ключей.

Соответствующие криптографические защитные меры могут противодействовать угрозам в отношении конфиденциальности и целостности информации. Криптографические защитные меры, такие как шифрование и аутентификация, требуют сохранение определенного материала, например криптографических ключей.

Для поддержки криптографических защитных мер может потребоваться одно или несколько средств, генерирующих, распределяющих и несущих ответственность за криптографический материал. Где это возможно, должны использоваться стандарты ИСО по распределению ключей в банковском деле.

Средства, обеспечивающие управление криптографическим материалом, должны подвергаться обеспечению физической защиты и управления доступом самого высокого уровня. Распределение ключей должно осуществляться по принципу разделенного знания для защиты безопасности системы.

Надежные криптографические практические приемы и эффективное планирование восстановления после бедствия благоприятствуют возникновению противоречивых требований. Необходимы тесные консультации лиц, отвечающих за восстановление после бедствия и криптографическую поддержку, чтобы гарантировать отсутствие компрометации между функциями.

Предоставление криптографического материала клиентам должно производиться так, чтобы минимизировать возможность компрометации. Клиент должен быть осведомлен о важности мер безопасности для криптографического материала. Взаимодействие с криптографической системой провайдера услуг, корреспондента или клиента должно допускаться только согласно полностью документированному гарантийному письму.

Качество безопасности, создаваемой криптографической продукцией, зависит от непрерывной целостности этих продуктов. И аппаратные, и программные криптографические продукты требуют защиты целостности, согласующейся с уровнем безопасности, которую они предназначены обеспечивать. Использование соответствующим образом сертифицированных интегральных схем, препятствующих порче корпусов и обнуления ключей отчасти упрощает защиту аппаратных систем по сравнению с программными средствами. Если обстоятельства позволяют, можно использовать криптографическое программное обеспечение продукции. Свойства, повышающие целостность систем, такие как самотестирование, необходимо использовать максимально.

Криптографическая продукция подчиняется различным правительственным положениям в отношении использования, импорта и экспорта. Положения местных властей в отношении использования, производства, продажи, экспорта и импорта криптографических устройств сильно различаются. Рекомендуется консультация с местным юрисконсультом или властями.

### 12.7 Распределение ключей

Как и в случае любой технологии существуют элементы, которые относительно просто реализовать и поддерживать, и другие, выполнение которых требует существен-

ных усилий. Одной из таких областей, которая требует тщательного планирования, обучения и точной реализации, является распределение криптографических ключей. К стандартам, рассматривающим распределение криптографических ключей, относится ИСО 11568.

Распределение ключей представляет собой часть криптографии, которая обеспечивает методы для 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 помочь достижению многих целей безопасности. Однако эти методы не имеют никакой ценности без надежного распределения криптографических ключей.

Основные функции распределения ключей состоят в предоставлении криптографических ключей, необходимых для криптографических методов, и защите этих ключей от любого вида компрометации. Конкретные процедуры и требования безопасности для распределения ключей зависят от вида криптосистемы, на которой основаны криптографические методы, характера самих криптографических методов, характеристик и требований безопасности компьютерной системы или сети, чья защита обеспечивается.

Наиболее важным для рассмотрения элементом является то, что распределение ключей должно быть достаточно гибким для эффективного использования в компьютерной системе или сети, и должно поддерживать требования безопасности системы. Услуги распределения ключей должны быть доступны в то время и в том месте, где они требуются, включая резервные площади. Распределение ключей должно быть частью плана организации по восстановлению после бедствий.

## 12.8 Неприкосновенность частной жизни

Финансовые учреждения обладают некоторой крайне значимой информацией об отдельных лицах и организациях. Законы и положения требуют, чтобы эта информация обрабатывалась и хранилась в соответствии с определенными правилами обеспечения безопасности и неприкосновенности частной жизни. Некоторые технические и бизнес-разработки, такие как сети, графическое представление документов, целевой маркетинг и современное использование информации между отделами, привели к озабоченности адекватностью обеспечения неприкосновенности частной жизни банков.

Финансовые учреждения должны пересматривать все законы и положения об обеспечении неприкосновенности частной жизни, такие как законы, связанные с кредитной информацией. Следует также быть в курсе нового национального законодательства о неприкосновенности частной жизни с помощью юридических контор банков, источников банковской индустрии или других независимых источников информации. Кроме того, банки, осуществляющие международные операции, должны знать региональные, международные и другие законы и положения обеспечения неприкосновенности частной жизни, которые имеют к ним отношения.

Финансовые учреждения должны анализировать свои операции с целью определения, обеспечивается ли адекватная защита информации об их клиентах и служащих. Необходимо разработать конкретные политики и процедуры, касающиеся сбора, использования и защиты информации. Эти политики и процедуры должны быть доведены до сведения соответствующих служащих. Политики и процедуры обеспечения неприкосновенности частной жизни должны рассматривать:

– сбор информации, для гарантирования сбора только информация, которая важна для обозначенной бизнес-потребности и является точной;

– обработку информации с целью обеспечения соответствующих ограничений доступа, включая определение того, кто должен иметь доступ к информации, контроль

качества для избежания ошибок при вводе данных или обработке, и защиту от непреднамеренного несанкционированного доступа;

– совместное использование информации, с тем чтобы оно происходило только посредством заранее определенных процедур, чтобы информация использовалась для целей, имеющих отношение к причинам ее первоначального сбора, и чтобы такое коллективное использование не вело к новым возможностям несанкционированного вторжения в частную жизнь другими сторонами;

– хранение информации с гарантией ее защиты от несанкционированного доступа;

– уведомление об использовании информации и наличие процедур, позволяющих лицу, чья информация находится на хранении, исправлять ошибки и вносить возражения относительно использования этой информации;

– надежное, ставшей ненужной, уничтожение информации, когда она больше не нужна.

Кроме того, электронные и другие формы контролирования действий служащих должны соответствовать нормативным требованиям, которые различаются в разных юрисдикциях. В дополнение к правам пользователей, защита персональной информации служащих и права из надлежащей правовой процедуры должны рассматриваться.

Финансовые учреждения должны рассмотреть вопрос проведения аудита по обеспечению неприкосновенности частной жизни. В ходе этого аудита оценивается, насколько хорошо организация выполняет защиту персональной информации, и рассматривает способы, которыми ИТ может решать проблемы обеспечения неприкосновенности частной жизни.

# 13 Дополнительные защитные меры

## 13.1 Поддержка

Поддержка защитных мер, включающая администрирование этих защитных мер, является важной частью программы обеспечения безопасности финансовой организации. Обязанностью руководства на всех уровнях является обеспечение того, чтобы:

– обязанности по поддержке защитных мер были четко установлены;

– выделялись ресурсы организации для поддержки защитных мер;

– защитные меры периодически проверялись и необходимость их использования повторно подтверждалась для гарантии непрерывности их действия;

– изменения аппаратных/программных средств и обновления системы ИТ не меняли или не сводили на нет намеченную эффективность существующих защитных мер;

– достижения технологий не способствовали появлению новых угроз или уязвимостей;

– защитные меры обновлялись и/или добавлялись новые защитные меры при появлении новых требований;

– политики безопасности пересматривались и корректировались или добавлялись новые политики на основе изменений защитных мер.

При условии выполнения выше описанных мероприятий поддержки, можно избежать неблагоприятного или дорогостоящего воздействия.

## 13.2 Соответствие требованиям безопасности

Проверка соответствия требованиям безопасности, также известная как аудит безопасности или анализ безопасности, является очень важным мероприятием. Проверка соответствия требованиям используется для обеспечения соблюдения и соответствия плану обеспечения безопасности информационных систем и гарантии поддержания эффективности соответствующего уровня информационной безопасности на протяжении срока службы системы или проекта ИТ. Это подразумевает стадии проектирования, разработки и реализации, а также применение обновлений, улучшений и исправлений. Следует также соблюдать осторожность при замене или ликвидации компонентов системы.

Проверки соответствия требований безопасности могут проводиться с помощью внутреннего и внешнего персонала (например, аудиторов), они часто основываются на использовании перечня контрольных вопросов, связанных с политикой безопасности системы или проекта ИТ. Проверки соответствия требований безопасности должны быть запланированными и интегрированными в разработки системы или проекта ИТ.

Дополнительным методом, который особенно полезен при определении соблюдения персоналом, занимающийся операционной поддержкой, и пользователями определенных защитных мер и процедур, являются выборочные проверки. Проверки должны проводиться для гарантии, реализации и правильного использования надлежащих защитных мер безопасности, где это уместно, защитные меры проверяются путем тестирования. В тех случаях, когда выясняется, что защитные меры не соответствуют плану обеспечения безопасности системы, необходимо уведомить об этом руководство участка, создать, реализовать и протестировать план корректирующих мер, а результаты проанализировать.

## 13.3 Мониторинг

Мониторинг представляет собой важный компонент плана обеспечения информационной безопасности. Мониторинг может служить для руководства показателем в отношении реализованных защитных мер – являются ли эти защитные меры удовлетворительными, и была ли внедрена программа поддержки защитных мер. Первоначальный план обеспечения безопасности можно будет сравнивать с результатами мониторинга с целью определения, какие защитные меры работают, а какие нет.

Многие защитные меры создают итоговые журналы регистрации связанных с безопасностью событий. Эти журналы должны периодически просматриваться и по возможности анализироваться, используя статистические методы с целью осуществления раннего обнаружения изменений тенденций и обнаружение 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 для послесобытийного анализа означает игнорирование важного механизма защитных мер.

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

# 14 Разрешение инцидентов

## 14.1 Менеджмент событий

Событие в области безопасности – это 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. Инцидент безопасности – это 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 безопасно неизбежно. Каждое событие должно расследоваться с целью определения, является ли оно инцидентом безопасности. Глубина этого расследования должна быть соразмерна ущербу, причиненному событием, или потенциальному ущербу, который могло бы нанести событие.

Обработка инцидентов предоставляет возможность реагирования на случайное или преднамеренное нарушение обычного функционирования системы ИТ. Необходимо разработать схему расследования инцидентов и представления отчетов о них, пригодная для всех систем ИТ и услуг организации. Эта схема должна включать представление отчетов группам ИТ и бизнес-группам для получения более широкого обзора возникновения 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 можно найти в ИСО/МЭК TR 18044 [9].

Основными задачами на время расследования инцидента информационной безопасности является реагирование на инцидент наиболее подходящим и эффективным образом и извлечение уроков из инцидента, чтобы в будущем можно было избежать аналогичных неблагоприятных событий. В некоторых ситуация может возникнуть необходимость, особенно для защиты репутации организации от критики неосведомленной недоброжелательной публики, обеспечения защиты конфиденциальности информации, имеющий отношение к инциденту безопасности.

Подготовленный план действий с заранее определенными решениями позволит организации осуществить реагирование за разумный срок с целью ограничения дальнейшего ущерба и, где это уместно, продолжить бизнес-деятельность посредством запасных мер. План обработки инцидентов должен включать требование по хронологическому документированию всех событий и действий. Это должно привести к определению источника инцидента. А этот фактор является предпосылкой для достижения второй цели, а именно, снижения будущих рисков посредством улучшения защитных мер.

Важно, чтобы также проводился и документировался анализ 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 вовремя?
- Что персонал предполагает делать иначе в следующий раз?
- Функционировал ли процесс анализа инцидента (обнаружение/реагирование/представление отчета) эффективно или его можно усовершенствовать?

– Существуют ли какие-либо меры управления для предупреждения повторного возникновения связанного с безопасностью события?

Ответы на эти вопросы и принятие решений по полученным данным снизят воздействия будущих инцидентов.

### 14.2 Расследования и судебный анализ

Для некоторых инцидентов требуется дополнительное расследование. Мошенничество, увеличенное во времени, недовольные служащие и некоторые правовые вопросы требуют расследования деятельности в системах ИТ. Для поддержки расследования может потребоваться собрание и анализ системных журналов, журналов систем обнаружения вторжений и иногда всех накопителей на дисках. Может потребоваться судебный анализ данных накопителя на дисках, включая поиск удаленных файлов, и другие виды детального анализа. Большинство организаций будут обладать только ограниченными внутренними возможностями для проведения таких расследований и анализа. Однако все программы обеспечения безопасности должны включать в себя некоторое минимальное обучение обработки свидетельства и план, касающийся того, кто будет проводить расследования, как они будут привлекаться, и какие виды судебного анализа они могут и будут выполнять. Реальные потребности будут значительно различаться для разных организаций и разных инцидентов.

### 14.3 Разрешение инцидентов

План разрешения инцидентов должен быть хорошо известен всем, кто будет принимать участие в разрешении инцидентов. В нем должны рассматриваться многие потенциальные вопросы: инциденты, происходящие во внерабочее время, потребности предоставления информации (как внутри организации, так и связь со средствами массовой информации и клиентам), планы резервирования и действий в чрезвычайных ситуациях, связь с поставщиками, включая бизнес-партнеров.

### 14.4 Аварийные проблемы

Для поддержания целостности во время чрезвычайных ситуаций, процессы безопасности не должны обходиться. Необходимы определенные процессы, позволяющие осуществлять исправление аварийных ситуаций только для разрешения производственных проблем, и необходимо создать процедуру как можно скорейшего возврата к обычным изменениям. В случае любого изменения, лица, осуществляющие их, включая персонал, осуществляющий поддержку в чрезвычайных ситуациях, должны документировать изменения. Наконец, необходима проверка всех аварийных изменений.

# Приложение А
# (информационное)

# Примеры документов

## А.1 Резолюция совета директоров по вопросу информационной безопасности

Постановили:

Информация является активом организации.

Как активы, информационные ресурсы и ресурсы обработки информации организации должны быть защищены от несанкционированного или ненадлежащего использования.

Главному исполнительному директору предписывается учредить программу обеспечения информационной безопасности, согласующуюся с разумной бизнес-практикой, с целью обеспечения надлежащей безопасности информационных активов организации.

## А.2 Политика информационной безопасности

Политика информационной безопасности
для
финансовой организации АВС

Финансовая организация АВС считает информацию в любой форме активом организации и требует наличия соответствующих защитных мер для обеспечения защиты этих активов от несанкционированного или ненадлежащего использования. Информация необходима для эффективной и результативной повседневной работы организации. Информация должна использоваться только для выполнения заданной цели – ведения бизне-операций финансовой организации АВС. Политика нашей организации состоит в предоставлении доступа к информации только на основе проверенного "принципа необходимого знания бизнеса" и отказывать в доступе всем другим.

Каждый старший управляющий организационной единицы финансовой организации АВС несет ответственность за поддержание конфиденциальности, целостности и доступности своих информационных активов и должен соблюдать все политики, стандарты и процедуры, которые опубликованы отделом информационной безопасности, касающиеся защиты информационных активов организации.

Все служащие имеют постоянную обязанность сознавать, поддерживать и соблюдать все политики, стандарты и процедуры организации, управляющие защитой информационных активов.

## А.3 Форма соглашения в части осведомленности служащих

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 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 целей выполнения моих рабочих обязанностей.

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

Я согласен немедленно сообщать о любом подозрительном поведении или ситуации, которые могут создавать угрозу безопасности информационных активов организации, моему руководителю.

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

Дата_____

_____ _____

Напечатанная фамилия служащего Подпись

_____

Свидетель (или руководитель)

## А.4 Экранные предупреждения при входе в систему

Это частная компьютерная система, доступ к которой ограничивается лицами с надлежащим санкционированием. Доступ уполномоченных сторон ограничивается теми функциями, которые им поручены для выполнения своих обязанностей. Любой несанкционированный доступ будет расследоваться и преследоваться судебным порядком. Если вы не являетесь санкционированным пользователем, немедленно отключитесь от системы.

В качестве альтернативы:

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

## А.5 Факсимильные предупреждения

***Платежное предупреждение***

ПРЕДУПРЕЖДЕНИЕ

Не рассчитывайте на эту пересылку для выплаты денег или инициирования других операций без независимой проверки ее полномочий

**Заявление о праве собственности**

Документы, включенные с этим факсимильным пересылочным листом, включают информацию организации АВС, являющуюся конфиденциальной и/или предназначенной для ограниченного круга лиц. Эта информация предназначена для использования адресатом, чье имя указано на этом пересылочном листе. Если вы не являетесь адресатом, обратите, пожалуйста, внимание на то, что любое раскрытие, фотокопирование, распространение или использование содержания этого факсимильного сообщения запрещено. Если вы получили это факсимильное сообщение по ошибке, пожалуйста, сразу же уведомите по телефону отправителя, чтобы мы могли организовать возвращение этих документов бесплатно.

## А.6 Информационное сообщение по информационной безопасности

***Предупреждение о компьютерном вирусе***

Согласно национальным 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***

Этот вирус пассивно находится на инфицированных компьютерах до инициирующей даты 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 (FAT) на загрузочном диске (гибком или жестком диске).

Восстановление данных пользователя с поврежденного диска является крайне трудным.

***Симптомы***

Сообщаемые симптомы включают:

– сокращение объема свободной/полной памяти на 2048 байт;

– гибкие диски, которые становятся непригодными или выводят странные символы при DIR командах.

Важно отметить, что вирус Микеланджело **не** выводит никаких сообщений на экране ПК в какой-либо момент времени.

***Риск инфицирования***

Вирус распространяется в результате:

– загрузки с инфицированной дискеты (даже если загрузка безуспешна) или

– загрузки с жесткого диска, в то время как инфицированная дискета находится в дисководе "A" и дверца дисковода закрыта.

Носители данных, которые используются на рабочих и домашних компьютерах, могут представлять риск с уровнем выше обычного.

## A.7 Форма принятия риска

***Принятие риска информационной безопасности***

Эта форма должна заполняться, только когда бизнес-процесс или система не соответствуют стандартам и политикам информационной безопасности и не отсутствует плана обеспечения соответствия данной политике в ближайшем будущем.

Подразделение_____ Номер запрашивающей организационной единицы_____

Руководитель подразделения_____ Название запрашивающей организационной единицы_____

Страница и номер пункта в политике/стандартах_____ Дата_____

Принятие риска запрашивается для (описание)_____
_____
_____
_____

Описание бизнес-процесса (приложить дополнительную документацию, если это уместно)
_____
_____
_____

Общее число операций за период_____

Полный денежный объем операций за период_____

Является ли временной интервал операций зависимым? (описание)_____

Затрагиваются ли счета в общей бухгалтерской книге?_____

Уровень руководства, получающего выходные данные_____

Значимость решений, основанных на выходных данных_____

Нормативные/юридически действительные встречные удовлетворения_____

Распространяются ли выходные данные среди клиентов? (описание)_____

Наивысшая классификация обрабатываемой информации_____

Описание системы, используемой для поддержки бизнес-процесса (приложить дополнительную документацию, если это уместно)_____
_____

_____

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_____

Количество пользователей_____

Географическое распределение пользователей_____

Описание интерфейсов с другими системами_____
_____
Требования к доступности _____
Работают ли на этом оборудовании другие приложения (описание)_____
_____

Поддерживаются ли системы центральной группой систем? Если нет, опишите механизмы 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 этого решения (другие рассмотренные альтернативы, дополнительные бизнес-факторы, то, как действуют другие компании и т. д.)
_____
_____
_____

Рекомендовано:_____ Дата_____
Руководитель подразделения

Проверено:_____ Дата_____
Ответственный за информационную безопасность

Комментарии:_____
_____
_____

Утверждено:_____ Дата_____
Руководитель с делегированными полномочиями

Номер документа принятия риска (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***

Этот договор имеет силу между _____ (в дальнейшем именуемым "Работником") и _____ (в дальнейшем именуемой "Компанией"). Стороны, намеренные принять на себя юридические обязательства, договариваются по поводу следующего:

*Объем обязательств по договору*

Работник принимает на себя обязательство осуществлять услуги для 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, отличие от обязанностей и обязательств, в прямой форме налагаемых на Работника в соответствии с данным договором, остаются неизменными.

Термины "дистанционное рабочее место" или "дистанционное место работы" должны означать место жительства Работника или любое удаленное рабочее помещение, утвержденное руководством Служащего.

*Условия договора*

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

*Аннулирование договора*

Участие Работника в качестве надомника является полностью добровольным и доступным только тем Работникам, которые будут сочтены подходящими для этого по единоличному усмотрению Компании. Права дистанционного присутствия не существует. Однако, предлагая свои услуги и будучи выбранным для выполнения дистанционного управления, Работник принимает на себя обязательство выполнять дистанционную работу в течении не менее "х" месяцев. Компания не будет нести ответственность за расходы, ущерб или потери, вытекающие из прекращения участия в дистанционной работе. Этот документ не является договором о найме и не может толковаться как таковой.

*Вознаграждение*

Рабочие часы, сверхурочная работа, надбавки за работу в неудобное время, отпуск: Работник согласен с тем, что рабочие часы, компенсация за сверхурочную работу, надбавки за работу в неудобное 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 уполномоченными лицами для целей, связанных с бизнесом, включая саморазвитие, обучение и выполнение задач. Служащий будет использовать телекоммуникационное оборудование строго в целях бизнеса. Компания не будет нести никакой ответственности за расходы на дистанционную связь, понесенные служащим при ведении личного бизнеса.

Компания по единоличному усмотрению может решить приобрести оборудование и соответствующие материалы 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 за Компанией.

Решение о перемещении или прекращении использования такого оборудования, данных и/или программных средств остается исключительно за Компании. Оборудование, приобретенное

для использования Работником, остается собственностью Компанией. Компания не несет ответственность за потери, ущерб или износ оборудования, находящегося в собственности Служащего.

Работник согласен определять рабочее место в помещении для дистанционного присутствия Работника с целью размещения и установки оборудования, которое будет использоваться во время работы. Работник должен поддерживать это рабочее место в сохранности и защищенном от рисков и других опасностей для Работника и оборудования. Компания должна одобрить площадь, выбранную в качестве дистанционного рабочего места служащего. Если происходят какие-либо изменения в первоначальном расположении на данном 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 опасностей от рисков, 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 процессу, понесенные Компанией, включая оплату юриста, если Компания выиграет процесс.

В случае сбоев 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 любых других обстоятельств, при которых Работник не сможет выполнять дистанционную работу, Работник знает, что ему может быть поручено выполнять другую работу и/или ему может быть отведено другое место по единоличному усмотрению Компании.

Освещение, обстановка, оборудование для охраны окружающей среды и обеспечения безопасности бытовых приборов, являющееся сопутствующим для используемого оборудования, программных средств и ресурсов Компании, должны использоваться по назначению и поддерживаться в безопасном состоянии, защищенном от дефектов и опасностей.

Работник согласен с тем, что всем данным, программным средствам, оборудованию, мощностям и ресурсам, принадлежащим Компании, должна обеспечиваться надлежащая защита. Данные, программные средства, оборудование и ресурсы, принадлежащие Компании, не должны использоваться для создания программных средств или личных данных. 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 Компании.

*Ответственность за ущерб*

Работник знает, что он отвечает за ущерб, 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 и всех исков, правопритязаний и ответственности (включая связанные с этим потери, расходы, издержки и оплату юристов), вытекающих или возникающих в связи с любым вредом причиненным людям (включая смерть) или собственности прямо или косвенно услугами, предоставляемыми в силу данного договора Работником, или в результате преднамеренной небрежности Работника, или его халатных действий, или недосмотра при выполнении обязанностей и обязательств Работника в соответствии с данным договором, за исключением тех случаев, когда эти иски, правопритязания и ответственность возникают исключительно из-за крайней небрежности или умышленного проявления халатности со стороны Компании.

*Прочие условия*

Работник согласен участвовать во всех исследованиях, опросах, отчетах и анализах, связанных с дистанционным присутствием, 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 собираться и становиться доступными общественности без идентификации личности Служащего.

Работник обязан соблюдать все правила, политики, практические приемы и указания Компании и условия данного договора и знает, что нарушение вышеупомянутого может привести к

недопущению к дистанционному присутствию и/или дисциплинарному взысканию вплоть до увольнения.

Я подтверждаю своей приведенной ниже подписью, что прочитал данный договор и знаю его содержание. Я подтверждаю, что мне была предоставлена возможность представить денный договор на рассмотрение моему адвокату перед вступлением в него.

Подпись Служащего: _____
Дата:_____

Дистанционное присутствие, или работа в другом месте, например, на дому, представляет собой назначение, которое предоставлено некоторым служащим при наличии взаимно выгодной ситуации.

Дистанционное присутствие – это не получение дохода работником, а скорее альтернативный метод удовлетворения потребностей данной Компании. У служащих нет "права" на дистанционную работу; Компания может прекратить соглашение в любое время.

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

1) Служащий согласен работать в следующем месте:

2) Служащий будет осуществлять дистанционное присутствие_____ дней в неделю.

3) Рабочие часы служащего будут такими:

4) Ниже приводятся задания, над которыми будут работать служащие на удаленном рабочем месте с ожидаемыми датами поставки:

5) На дистанционном рабочем месте служащим будет использоваться следующее оборудование:

6) Ниже приводится согласованный механизм оперирования телефонными звонками, сделанными дистанционным работником с удаленного рабочего места по делам Компании:

7) Служащий согласен получать от_____ все ресурсы, необходимые для работы в альтернативном месте; разного рода наличные выплаты за ресурсы, регулярно предоставляемые в офисе Компании, обычно не будут возмещаться.

8) От служащего будет требоваться совершение регулярных посещений _____Центра для прохождения обучения и совещаний с командой и начальником.

Я просмотрел представленный выше материал с _____ до его участия в программе Компании по.

Дата:_____ Подпись инспектора_____

Обсуждался со мной приведенный выше материал.

Дата:_____ Подпись Работника_____

# Приложение В
# (информационное)

# Пример анализа безопасности веб-сервисов

## В.1 Высокоуровневый анализ безопасности

### В.1.1 Общий обзор

Подобно политикам, которые могут быть очень высокого уровня или быть крайне детализированными, анализ риска может быть завершен с различными степенями детализации. В данном подпункте предоставляется обсуждение высоких уровней веб-сервисов, новой технологии, которая имеет значение для многих компаний, предоставляющих финансовые услуги и других компаний, использующих Интернет для бизнеса. Этот пример анализа предназначен только в иллюстративных целях и не должен рассматриваться как конкретная рекомендация в отношении безопасности. Как отмечается на протяжении данного документа, каждая организация должна составить свое собственное определение риска и безопасности на основе своих конкретных политик и потребностей бизнеса.

Веб-сервисы (WS) – это общий отраслевой термин для новой серии стандартов 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, к которым могут получать доступ скорее другие компьютеры, чем человек визуально через браузеры. Веб-сервисы являются достаточно мощными и способными обеспечивать взаимодействие через системы, организационные единицы и компании.

Основными компонентами веб-сервисов являются:

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

Существует большое число "определений"того, что составляет веб-сервис, но обычно общепринятым определением является информационная услуга, которая раскрывает информацию через простой протокол доступа к объектам (SOAP) стандарта W3C [20] Клиент интерфейса SOAP должен знать, как получить доступ к этим информационным услугам. Этот 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

Безопасность веб-сервисов должна учитывать сервер приложений, поддерживающий сервис, описание сервиса, хранилище сервиса, клиента, использующего сервис, и протокол связи. Различными поставщиками и консорциумами была разработана Структура безопасности веб-сервисов и ряд спецификаций. Кроме того, можно использовать универсальное решение проблемы веб-безопасности, SSL, для обеспечения определенной безопасности веб-сервисов. В этом пункте будут обсуждаться дополнительные подробности обеспечения безопасности веб-сервисов.

### В.1.3 Стандарты безопасности

SOAP и WSDL представляют собой определения обмена сообщениями и сервиса, соответственно, которые должны быть защищены для каждой из бинес-услуг, в которой они используются. Однако в настоящее время они не обозначают совершенное средство обеспечения целостно-

сти данных, аутентификации источника или услуг конфиденциальности для приложений веб-сервисов. Ожидается появление требования, и SOAP имеет структуру расширения, предусматривающую добавление элементов безопасности и протоколов стандартизованном виде. В данном подпункте приводится общий обзор некоторых стандартов безопасности, связанных с веб-сервисами.

Язык разметки для систем утверждения безопасности (SAML) определяет основанную на языке XML структуру обмена информацией по 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 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, позволяющих или запрещающих субъекту доступ к компьютерным ресурсам. Развитие SAML тщательно контролируется индустрией, которая надеется, что он станет стандартным средством передачи регистрационной информации для веб-сервисов основанных на SOAP. В настоящее время у SAML существует связующее описание SOAP.

Безопасность веб-сервисов представляет собой предлагаемую совокупность расширений SOAP, позволяющих операциям веб-сервисов обладать целостностью и конфиденциальностью. Безопасность веб-сервисов имеет целью обеспечение целостности и конфиденциальности посредством передачи маркеров доступа, целостности сообщений и конфиденциальности сообщений. Предлагаемая компаниями Микрософт и IBM безопасность веб-сервисов и ответственность позднее перешла к OASIS (организации по продвижению стандартов для структурированной информации).

Шифрование на языке XML – это спецификация W3C, метода передачи информации на языке XML стандартным зашифрованным образом. Шифрование XML дает возможность шифровать и дешифровать цифровое содержание, включая в себя сам XML документ, на элементном, но не на атрибутивном уровне. Спецификация также позволяет осуществлять безопасную передачу информации о ключе для дешифрования содержания получателем документа на XML.

Подпись на языке XML – это проект рекомендации объединенной группы IETF (проблемной группы проектирования Интернет) и W3C по представлению информации цифровой подписи в документах на языке XML. "Подписи на языке XML обеспечивают целостность, аутентификацию сообщения и/или услуги аутентификации подписавшего лица для данных любого типа, расположенных в XML, включающем в себя подпись, или где-то в другом месте". Подпись на языке XML – это основной стандарт, на который делается ссылка в других стандартах безопасности, включая шифрование на языке XML, SAML и безопасность веб-сервисов.

Liberty Alliance Project – это консорциум, возглавляемый крупными фирмами, планирующий позволить совместимое открытое использование технологий интегрированного идентификатора. Интегрированный идентификатор позволяет потребителю использовать единый признанный идентификатор во многих организациях. Этот потребитель может использовать одну и ту же надежную информацию идентификатора в группе различных организаций, и этот потребитель не должен представлять новый идентификатор, мандаты идентификации собственности.

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

## B.2 Стандарты веб-сервисов

### B.2.1 Общий обзор

Стандарты для веб-сервисов развиваются быстро. Тремя главными участками работы, 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 виде, позволяет пользователям находить и активи-

зировать сервисы. Существует большое число используемых стандартов безопасности для обеспечения услуг определения подлинности, шифрования, подписи и утверждения 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

Внедрение веб-сервисов, по крайней мере с общей точки зрения, требует определенного изучения риска или угроз, с которыми сталкиваются веб-сервисы, и мер безопасности по уменьшению этих угроз. Для такого анализа рассмотрите рисунок B.1 и относительно простой веб-сервис (WS1), имеющий дело с клиентами во всей сети организации. На этом рисунке четыре клиента могут запрашивать услуги веб-сервиса WS1. Отметьте, что эти клиенты могут быть также веб-сервисами по собственному праву, 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 расчета месячных платежей.

Клиент S2 расположен на ближайшей сетевой шине, возможно, в том же информационном центре, что и WS1. Клиент S3 тоже находится во внутренней сети компании, но, возможно, гораздо дальше, может быть, в филиале в другом штате или в другой стране. Клиент S4 находится в демилитаризованной зоне (DMZ), соединенной с Интернетом, и имеет определенный уровень связи с Интернетом и внутренней сетью компании. Наконец, возможно, что внутренний сервис типа WS1 может быть доступен клиентам в Интернете, таким как S5.

### B.2.3 Обеспечение безопасности

Требования безопасности для веб-сервиса WS1 обычно могут быть сведены в несколько категорий в отношении общих угроз. Во-первых, существует конфиденциальность входных данных при запросе сервиса 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 быть требования целостности данных без требований конфиденциальности.

Хотя требования безопасности для WS1 являются простыми, рассмотрение для построения решения может быть сложным. Например, безопасная аутентификация между клиентом веб-сервиса и сервером веб-сервиса может осуществляться с помощью паролей, сертификатов и, возможно, другими методами. Хотя сертификаты обеспечивают значительную степень безопасности, другие функциональные назначения – эффективность, выравнивание нагрузки, обработка отказа – могут делать их внедрение проблематичным. Пароли, хотя и являются менее безопасными при некоторых обстоятельствах, могут быть достаточными в других сценариях. Например, для клиента веб-сервиса, обращающегося к веб-сервису, работающему на той же аппаратуре, пароли, проходящие через память машины, могут обеспечивать достаточную безопасность. Если клиенты веб-сервиса располагаются дальше от сервиса, могут потребоваться шифрованные пароли. Пароли могут шифроваться на прикладном уровне, используя стандарты безопасности веб-сервисов, или на транспортном уровне, используя SSL, или на сетевом уровне, используя IPSEC (протокол безопасности IP). Требования обеспечения конфиденциальности входных и выходных данных могут аналогичным образом выполняться на прикладном уровне, на транспортном уровне или на сетевом уровне.

Отметьте, что требования аутентификации конкретно адресуются 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.

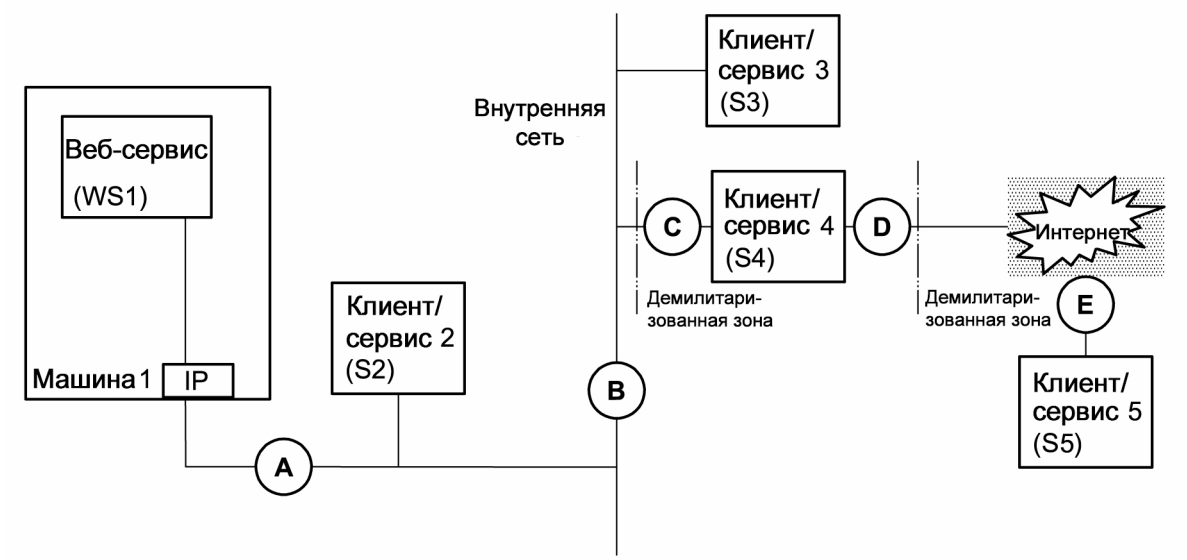



Рисунок В.1 - Общая модель веб-сервисов

### В.2.4 Анализ угроз

Угрозы WS1 включают в себя неправильное использование сервисом, 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 генерировать сообщение об ошибке, если данные ввода-вывода выходят за ожидаемые пределы. С отказом от обслуживания можно справиться, 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 сервис. 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 очень защищенным; в противном случае он провоцирует некое лицо, создающее 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 он является просто калькулятором.

### В.2.5 Решения

Решения по обеспечению требований 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 этих случаях клиент и сервис расположены близко друг от друга 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, разумно предположить, что конфиденциальность данных и аутентификация паролей основываются просто на их изоляции от остального мира.

По мере удаления от WS1 сложность возрастает. Между клиентом S3 и WS1 запросы в обслуживании проходят по более широкой сети, открывая больше возможностей проверки запросов и больше точек, где может быть создан и введен несанкционированный запрос. Таким образом, между S3 и WS1 требуется дополнительная защита. Как описывалось ранее, это может быть аутентификация на основе сертификатов и это может быть IPSEC между аппаратными средствами S3 и аппаратными средствами WS1.

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

Наконец, для запросов веб-сервисов извне организации в S5, входящие запросы, вероятно, потребуют сложного решения. Идентификационная информация может быть защищена на прикладном уровне и безопасным образом передана через Интернет, через демилитаризованную зону в WS1, так чтобы WS1 мог определить, уполномочен ли S5 для запроса на обслуживание и услуги. 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, чтобы удостовериться, что данные находятся в пределах соответствующих параметров, затем вновь выполнено шифрование для передачи данных в WS1, где информация опять будет дешифрована. Подобным образом весь запрос веб-сервера может быть дополнительно зашифрован на транспортном или сетевом уровне для промежуточного сервиса (возможно, S4) в демилитаризованной зоне, который вновь создаст запрос WS1, вероятно, немного в ином формате, с тем, чтобы интерфейс WS1 никогда не подвергался воздействию вне 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 в аутентификации и конфиденциальности. Существует также множество мест в типичной 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.

Существует также много других соображений. Качество функционирования между клиентом и сервером часто бывает критичным. Обработка отказа, резервирование, восстановление и аналогичные вопросы непредвиденных обстоятельств могут делать некоторые контрмеры более привлекательными. Инструментальные средства разработки веб-сервисов, имеющиеся в различных компаниях, обеспечивают различные виды поддержки для стандартов SSL и стандартов безопасности веб-сервисов; ваше инструментальное средство может не поддержать повторное использование SSL сеанса на основе сертификатов. Поскольку сервер приложений может иметь различные возможности по отношению к стандартным инструментальным средствам, результаты могут быть различными.

## Приложение С
## (информационное)

## Иллюстрация оценки риска

### С.1 Табличная форма оценки риска

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Уязвимость: Персонал<br>Идентифицировать уровень риска, вытекающего из угрозы следующего: | Риск денежных потерь | | | Риск уменьшения продуктивности | | | Риск для репутации | | |
| 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 поставки или неправильно адресованная поставка 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 |
| Уязвимость: Помещения и оборудование<br>Идентифицировать уровень риска, вытекающего из угрозы следующего: | Риск денежных потерь | | | Риск уменьшения продуктивности | | | Риск для репутации | | |
| 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 поставки или неправильно адресованная поставка 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 |
| **Уязвимость: Приложения**<br>Идентифицировать уровень риска, вытекающего из угрозы следующего: | Риск денежных потерь | | | Риск уменьшения продуктивности | | | Риск для репутации | | |
| Несанкционированное раскрытие, изменение или разрушение информации | В | С | Н | В | С | Н | В | С | Н |
| Непреднамеренное изменениеили разрушение информации | В | С | Н | В | С | Н | В | С | Н |
| Отсутствие поставки или неправильно адресованная поставка 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 |
| **Уязвимость: Системы связи**<br>Идентифицировать уровень риска, вытекающего из угрозы следующего: | Риск денежных потерь | | | Риск уменьшения продуктивности | | | Риск для репутации | | |
| 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 поставки или неправильно адресованная поставка 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 |
| **Уязвимость: Программные средства среды и операционные системы**<br>Идентифицировать уровень риска, вытекающего из угрозы следующего: | Риск денежных потерь | | | Риск уменьшения продуктивности | | | Риск для репутации | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 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 поставки или неправильно адресованная поставка 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 содействия в оценке риска бизнес-функций. Она разделена на пять зон уязвимости:

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

### С.2.2 Потенциальные угрозы

Под названием каждой зоны уязвимости в табличной форме оценки риска перечислены четыре потенциальные угрозы, которые подлежат оценке:

1) несанкционированное раскрытие, изменение или разрушение информации;
2) непреднамеренное изменение или разрушение информации;
3) отсутствие поставки или неправильно адресованная поставка 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 риска – денежные потери, 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 денежных потерь в доходе или капитале может возникать из-за проблем с услугами, информационными системам или поставкой продукции. Степень этого риска является функцией внутренних средств защиты, информационных систем, честности служащих и рабочих процессов.

Риск, относящийся к доходам, капиталу и бизнес-репутации, вытекающий из негативного общественного мнения, может оказать влияние на способность финансовых учреждений устанавливать новые взаимосвязи или услуги или поддерживать существующие. Риск может подвергнуть организацию судебному процессу, финансовым потерям или дальнейшему ущербу для репутации. Продолжающийся риск доходам или капиталу из-за нарушения законов, правил, положений, предписанных практических приемов или этических стандартов или из-за несоответствия им может подвергнуть финансовую организацию штрафам, гражданско-правовым денежным санкциям, возмещению убытков и лишению контрактов.

В данном стандарте используются следующие степени риска:

– высокая (В) – значительные денежные потери, уменьшение продуктивности или ущерб для репутации, вытекающие из угрозы, появляющейся вследствие соответственной уязвимости;

– средняя (С) – незначительные происходящие денежные потери, уменьшение продуктивности или ущерба для репутации;

– низкая (Н) – минимальная возможность денежных потерь, уменьшение продуктивности или ущерба для репутации или полное ее отсутствие.

### 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 предприятию необходимо:

– проанализировать, что означает каждая из потенциальных угроз в табличной форме для оцениваемой деловой функции;

– задать вопрос, каким образом и кто будет подвергаться риску и какая степень риска будет вытекать из каждой потенциальной угрозы, происходящей вследствие каждой уязвимости.

При определении степени риска не существует абсолютных правил. Установление пределов денежных средств, пределов человеко-часов и наихудших при принятии решения событий быть полезным. Когда возникают сомнения при анализе потенциальных угроз, представить, что произойдет наихудшее событие, и выберите 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, первая угроза в таблице под заголовком "Помещения и оборудование" может быть проанализирована следующим образом.

1) Если лицо со стандартным доступом раскрывало информацию о ваших помещениях и оборудовании (т.е. служащий отдела раскрывает комбинацию сейфа отдела, содержащего ценности или конфиденциальную информацию), могут ли возникнуть денежные потери, уменьшение продуктивности или ущерб для репутации учреждения?

2) Будет ли уровень потерь и/или ущерб для репутации высоким, средним или низким?

Идентифицированные угрозы (т. е. служащий отдела раскрывает комбинацию сейфа отдела, содержащего ценности или конфиденциальную информацию) должны быть документированы вместе с использованным логическим обоснованием. Для некоторых бизнес-функций может быть уместен ответ "неприменимо" (N/A) для какой-либо угрозы вследствие некоторой уязвимости или всей категории уязвимостей. Когда такое происходит, должно документироваться логическое обоснование, лежащее в основе решения, а документация должна сохраняться в файле с заполненной табличной формой.

Когда угрозы идентифицированы, возникает выбор принятия рисков, при условии, что для этого имеются полномочия, или уменьшать риски. Риски могут быть уменьшены путем передачи риска (страхование), принятия мер в отношении рисков (снижение) путем применения средств управления безопасностью или избежания риска посредством устранения источника угроз путем изменения бизнес-цели.

### С.3 Таблица оценки риска

Для каждой категории риска нужно ввести степень риска, – высокая (В), средняя (С) или низкая (Н) – связанная с каждой уязвимостью. Произведя оценку каждой категории риска, нужно установить общий риск для каждой уязвимости. Когда таблица будет заполнена, следует выбрать соответствующие средства управления.

| | Категория риска | | | |
|---|---|---|---|---|
| Уязвимости | Денежные потери | Уменьшение продуктивности | Ущерб для репутации | ОБЩИЙ РИСК |
| Персонал | | | | |
| Помещения и оборудование | | | | |
| Приложения; | | | | |
| Системы связи | | | | |
| Программные средства среды и операционные системы | | | | |

## С.4 Описание таблицы оценки риска

### С.4.1 Краткий обзор

Таблица оценки риска используется для показа комбинированной степени риска для каждой уязвимости. Три категории риска перечисляются сверху таблицы, а пять зон уязвимости – в левой колонке таблицы.

Таблица оценки риска заполняется путем установления комбинированного уровня риска для каждой из пяти зон уязвимостей. Комбинированная степень риска должен быть получен из четырех угроз, ранее идентифицированных в табличной форме оценки риска в С.2.2.

### С.4.2 Инструкции по таблице риска

Для комбинирования риска для каждой категории, нужно изучить степени риска, обведенные кружком для каждой уязвимости в табличной форме оценки риска (смотри С.1С.1). Нужно взять каждую категорию риска по отдельности и определить, каким будет комбинированная степень риска для четырех угроз (смотри С.2.2). Запишите степень риска в таблице оценки риска.

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

Учтите, что при определении комбинированных степеней риска для каждой уязвимости не существует абсолютных правил. Однако нужно принимать во внимание следующее:

- возможность или вероятность возникновения угрозы. Угрозы с большей вероятностью возникновения должны оказывать более существенное влияние на устанавливаемую степень риска. Угрозы с наименьшей вероятностью возникновения должны оказывать менее существенное влияние;
- угрозам, имеющим более существенное отношение к оцениваемой бизнес-функции, должна придаваться большая значимость при установлении степени риска;
- следует проявлять осторожность при оценке степени риска и в случае сомнения выбирать более высокую степень риска.

В качестве примера оценки общего риска угрозе отсутствия поставки или неправильно адресованной поставки информации может придаваться большая значимость при выборе степени общего риска, потому что отсутствие поставки может считаться более значимым для анализируемой бизнес-функции, чем несанкционированное раскрытие этой информации.

### С.4.3 Выбор средств управления

Выбор защитных мер безопасности обеспечивает учреждению непосредственное управление риском, который он принимает. Учреждению нужно оценить, насколько запланированные и существующие защитные меры снижают риск, идентифицированный при анализе риска, определить дополнительные защитные меры, которые имеются в наличии или могут быть разработаны, разработать архитектуру безопасности ИТ и определить ограничения различных типов (смотри 8.3 – 8.7). Затем должны быть выбраны соответствующие и обоснованные защитные меры для снижения оцененных рисков до приемлемого уровня. Дополнительные подробности о выборе защитных мер можно найти в ИСО/МЭК ТО 13335.

### С.4.4 Ранжирование воздействия и вероятности

Для степени вероятности и воздействия используется шкала от 1 до 9. в данном подпункте объединяется, что это означает на практике, устанавливая обычную оценку масштаба вероятности и определяя воздействие под каждой из шести основных категорий Структуры Рисков Предприятия. Хотя это дает ощущение "измеренности", значения должны рассматриваться как руководство по порядку величины, а не как абсолют.

Для вероятности принято следующее ранжирование:

1) **пренебрежимо малая** – раз в 1000 лет или меньше;
2) **крайне маловероятная** – раз в 200 лет;
3) **очень маловероятная** – раз в 50 лет;
4) **маловероятная** – раз в 20 лет;
5) **возможная** – раз в 5 лет;
6) **вероятная** – ежегодно;
7) **очень вероятная** – ежеквартально;
8) **ожидаемая** – ежемесячно;
9) **ожидаемая с уверенностью**– еженедельно.

Очень приблизительно каждая из них в четыре раза более вероятна, чем предыдущая.

Ниже приведен масштаб воздействия по каждому из шести основных именований в структуре. Не каждый блок таблицы заполнен, но она дает общую картину. Некоторым оценкам риска могут потребоваться другие определения, но используемые степени должны быть в общих чертах сходными.

Таблица С.1 - Оценка риска

| Рейтинг | | Описание | Репутация | Операционный | Безопасность | Правовой | Финансовый | Стратегический |
|---|---|---|---|---|---|---|---|---|
| НИЗКИЙ | 1 | пренебрежимо малое | | | Локальный пароль к не секретным данным раскрыт, но не использован | | <$100 | |
| | 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 | ~$1 000 | |
| | 3 | незначительное | "Стандартные" язвительные высказывания в национальной прессе или размещенные в Интернете о банковской системе, например, письмо читателя | Временное невыполнение обслуживания (~1 ч.) для одного члена системы; проблемы, оказывающие ограниченное влияние на клиентов | Утечка или компрометация незначительного количества текущей информации | Идентифицирована поправимая возможность несоответствия | ~$5 000 | Политики или стандарты не поддерживаются |
| СРЕДНИЙ | 4 | заметное | Внимание национальной прессы или радио, например, плохой отзыв в DD схеме | Эксплуатационные проблемы, оказывающие воздействие на весь клиринг | Злоупотребление законными привилегиями доступа | Неспособность предоставить данные, требуемые законом, например, согласно закону Сэрбэйнс-Оксли | ~$20 000 | |

| Рейтинг | | Описание | Репутация | Операционный | Безопасность | Правовой | Финансовый | Стратегический |
|---|---|---|---|---|---|---|---|---|
| СРЕДНИЙ | 5 | существенное | Серьезная критическая статья в прессе или документальная передача по радио или по телевизору, склонная рассматриваться как исходящая из заслуживающего доверия источника | Временное невыполнение обслуживания для многих членов системы или длительное невыполнение обслуживания (до целого 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 | ~$100 000 | Политики или стандарты не существуют |
| | 6 | очень существенное | Публичная критика со стороны регулятивного или отраслевого органа | Член системы не способен работать с клирингом | Успешное мошенничество мелкого - среднего масштаба | Начало полицейского или регулятивного расследования; регулятивное вмешательство, иск удовлетворен | ~$1 000 000 | |
| | 7 | большое | Ведущая новость во многих газетах и/или в 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) | ~$10 000 000 | Управленческий контроль скомпрометирован |
| ВЫСОКИЙ | 8 | очень большое | Государственное вмешательство или сравнимые политические последствия | Невыполнение клиринга в течение всего рабочего дня | Клиринговая система взломана и серьезно скомпрометирована | Судебное преследование, возбужденное против клиринговой палаты (успешное) | ~$100 000 000 | |
| | 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 | ~ $1 000 000 000 | Будущее существование клиринговой палаты под сомнением; платежная индустрия скомпрометирована |

Отметьте, что оценка приводится для **чистого**, а не для **общего** риска. Другими словами, их внимание должно быть уделено влиянию **при наличии имеющихся мер управления**. Обычно, наличие предупреждающих мер управления снижает вероятность возникновения события, но не влияет на его воздействие; мер управления, специально направленные на уменьшение воздействия, обычно не влияют на вероятность.

**Подверженность или "значимость"**

"Отмеченная" для воздействия и вероятности, следующая модель используется как средство определения подверженности. В нее включены пять уровней; на практике все, оценивающееся как уровень 1, не заслуживает дальнейшего анализа, а со всем, оценивающимся как уровень 5, следует разбираться немедленно, а не продолжать оценку риска! Так что в сущности мы получаем шкалу с тремя отметками.

Обозначение закраски:

Незащищенность от воздействия/значительность

| | |
|---|---|
| Критическая – 5 | 5 |
| Значительная – 4 | 4 |
| Существенная – 3 | 3 |
| Незначительная – 2 | 2 |
| Пренебрежимо малая – 1 | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Влияние | **9** | 3 | 3 | 4 | 4 | 4 | 5 | 5 | 5 | 5 |
| | **8** | 3 | 3 | 3 | 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, тем больше усилий нужно затратить на анализ и управление риском. На этой стадии не стоит слепо следовать "оценочной" системе; самым необходимым является определение основных проблем риска, которые будут рассматривать руководство – в любом порядке, который оно считает уместным, на основе всей имеющейся информации, включая подверженность риску, но никоим образом 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, обычно существует четыре образа действий, из которых можно делать выбор. Эти образы действий таковы:

– **Избежание** – Как подразумевает название, это просто означает устранение источника угрозы или изменение бизнес-цели с целью удаления риска. Хотя это кажется идеальным способом обращения с риском, он, по-видимому, применим лишь в редких случаях. "Нет риска, нет бизнеса!" Например, вы можете избежать риск быть сбитым машиной, никогда не выходя из дома, но значительная часть жизни будет проходить мимо вас. В качестве примера, более близкого к бизнес-операциям: мы можем предотвращать воздействия несостоятельности третьей стороны, не используя третью сторону – в этом случае у нас, вероятно, не останется достаточно бизнеса для работы! Однако в тех случаях, когда риска можно реально избежать, это часто дешевое и долговременное решение.

– **Принятие мер** – Принятие мер в отношении риска является тем, что мы склонны делать наиболее часто и что в определенном смысле подразумевается в принятом нами *образе действий*, который звучит как "разработай план действий". Это просто означает выполнение действий, которые уменьшат вероятность материализации риска или ограничат эффект события и таким образом уменьшат его воздействие. Примеры этого многочисленны и, в значительной степени, 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** – Распределение риска означает возложение основной части влияния на третью сторону. Классическим способом достижения этого является страхование. Несомненно, распределение редко достигается без определенных текущих расходов! Например, мы можем распределить нашу ответственность за выдачу некачественной консультации путем профессиональной компенсационной политики – за определенную цену. Риски иногда можно распределить третьим сторонам через договорное соглашение (как ответственность), хотя способность третьей стороны обращаться с последствиями сама собой может представлять риск!

– **Принятие** – Последней возможностью является простое принятие риска; быть осведомленным о том, что риск может появится, но, оценив расходы и возможность удаления трех других вариантов, принять решения о том, что величина риска перевешивается потенциальными выгодами работы с ним. Например, мы можем решить принять риск вынужденного физического доступа в наши помещения преступников, с огнестрельным оружием потому, что стоимость физических мер безопасности очень высока и их установка неблагоприятно повлияет на прием, который мы оказываем нашим членам.

Конечно, возможно использовать смешанные подходы к определенным рискам, – это не является точной наукой – так что развивая пример доступа вооруженных преступников, в то время как мы, приняв некоторую степень риска, мы можем принимать меры в отношении меньших угроз (таких как люди, случайно зашедшие с улицы), используя невооруженную охрану, выбирать ограничение их последствий, добавляя доступ с клавишным вводом личного идентификационного номера к ключевым зонам или сужая функции, которые могут осуществляться (при условии угрозы) на основных системах, или, возможно, передавать часть риска путем оформления страхования жизни наших служащих.

**Остаточные риски**

Нужно определить, какие действия и мероприятия по мониторингу следует предпринимать для осуществления менеджмента остаточных рисков, и определить ответственность за все действия.

# Приложение D
# (информационное)

# Технологические средства управления

## D.1 Аппаратные средства

### D.1.1 Средства управления конечной системой

Большинство организаций сегодня использует некоторую комбинацию настольных ПК и переносных ПК в качестве основных ориентированных на пользователей систем. Эти конечные системы используют различные операционные системы, хотя преобладающее большинство из них исходит от одного поставщика. Кроме того, эти машины дополняются или в некоторых случаях заменяются небольшими персональными цифровыми секретарями (PDA). 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 на базе ПК. Другие работники предприятия часто используют Интернет-технологию для приложений, таким образом предоставляя доступ для пользования персональным цифровым секретарям и сотовым телефонам.

В случае любой конечной системы первой стадией охвата являются связанные с безопасностью установки в операционной системе также. Неиспользуемые и ненужные подсистемы, как базы данных и функции операционной системы, должны быть отключены и удалены. Другие функции должны быть ограничены до минимума, необходимого для надлежащего функционирования пользователя. Кроме того, у предприятия должен быть определенный механизм использования патчей для систем и распространения обновлений при наличии у поставщиков, как для операционной системы, так и любых приложений, работающих на конечных системах. Например, было выявлено несколько проблем с макросами от компании Микрософт в офисном пакете.

Помимо операционной системы предприятие должно рассмотреть роль конечных систем и обдумать, будут ли необходимы дополнительные свойства, подобные антивирусным программам, обнаружению вторжения, предупреждению вторжения, межсетевым экранам и виртуальной частной сети, для пользователей предприятия. Во многих случаях внешние системы безопасности данной организации (которые определены в пункте 11.5) будут обеспечивать свойства, подобные антивирусным программам, межсетевым экранам, обнаружению и предупреждению вторжения. Однако при наличии мобильных систем и с ростом бизнес-партнерства и аутсорсинга, дублирование этих свойств в мобильных системах и потенциально на персональных цифровых секретарях и настольных ПК имеет смысл для традиционной многоуровневой защиты. Например, мобильный ПК пользователя, подсоединенный к широкополосной связи из дома и использующий виртуальную частную сеть предприятия, становится каналом для атаки и временным устройством периметра, требующим обеспечения такой же безопасности, как другие устройства периметра.

### D.1.2 Средства управления серверными системами

Подобно конечным системам серверные системы нуждаются в применении и внутренних средств управления на уровне операционной системы, и внешних средств управления. Для серверов часто требуются функциональные возможности и подсистемы, которые не требуются для конечных системами. Поскольку на сервере может работать база данных, веб-сервер, FTP сервис и/или много других функций, эти серверы имеют более значительный потенциальный интервал уязвимости. Эти серверы требуют предоставления доступа к другим устройствам, которые не всегда могут быть надежными. Кроме того, подобно конечным системам необходимо предусмотреть тестирование, обновление и менеджмент систем, по мере выпускаю новых патчей и версий. Со-

ответствующий процесс включет в себя тестирование нового патча в непроизводственной среде перед установкой патча на производственных системах.

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

Помимо операционной системы, определенное внимание должно быть уделено антивирусным программам, обнаружению вторжения и межсетевым экранам на сервере и вокруг него. Это может принимать форму размещения сервера в безопасной зоне за межсетевым экраном и использование системы обнаружения вторжения на базе сетевого устройства, или все три сервиса безопасности могут быть использованы на самом серверном хосте. Разнообразие организационных, сетевых вопросов и вопросов безопасности обусловливает оценку и определение того, какие средства контроля уместны для каких серверных систем.

### D.1.3 Средства управления универсальными вычислительными машинами

Универсальные вычислительные машины создаются лишь немногими производителями для обработки больших объемов данных. В результате универсальные вычислительные машины склонны рассматриваться как более надежные и более мощные, чем другие ИТ системы обработки ИТ. Тем не менее, менеджмент универсальных вычислительных машин должен осуществляться, используя такие же принципы безопасности, как для других систем. Основная операционная система должна быть защищена, и необходимо рассмотрены дополнительные меры помимо операционной системы. Обычно универсальная вычислительная машина содержит наиболее ценную информацию организации и бизнес-правила, поэтому она размещается в центре многоуровневой сетевой архитектуры безопасности. Каждому пользователю присваивается соответствующий идентификатор с ограниченными функциональными возможностями; несколько членов персонала осуществляют административное управление универсальной вычислительной машиной. Как и в случае с другими системами, в качестве части средств управления безопасностью универсальной вычислительной машины необходимо внимательно рассмотрено разделение обязанностей.

### D.1.4 Средства управления другими аппаратными системами

Другие аппаратные устройства и системы имеют аналогичные проблемы, и они должны быть оценены перед развертыванием производства в организации. Эти устройства могут быть специальными шифровальными системами, новыми типами аппаратных средств, которым оказывают предпочтение многие поставщики межсетевых экранов и систем обнаружения вторжения, или сетевыми аппаратными средства, такими как маршрутизаторы и коммутаторы. Во всех случаях продукцию необходимо оценить, чтобы понять лежащую в его основе операционную систему, и эта операционная система должна быть защищена для предотвращения легких атак. Кроме того, большое значение имеет расположение этих устройств по отношению к внутреннем сетевым соединениям, межсетевым экранам, системам поиска вирусов и обнаружения вторжения.

## D.2 Программные средства

### D.2.1 Веб-серверы

Веб-серверы – это очень распространенное и часто используемое приложение, предназначенное главным образом для распределения веб-страниц для пользователей. Приложение может варьироваться от очень простых, предоставляющих только фиксированные страницы информации – до очень сложных - предоставляющих многостраничные документы с поддержкой сценариев, активных программных машинных команд и многого другого. Организации должны определить, какая степень сложности им нужна, и соответствующие связи между Интернетом, веб-сервером (веб-серверами) и внутренними данными. Обычно, финансовые учреждения настаивают на трехзвенной архитектуре с межсетевым экранами, обеспечивающими границу между Ин-

тернетом и веб-сервером и между веб-сервером и внутренними данными. Многозвенные архитектуры, которые разделяют дополнительные уровни приложений или бизнес-логики, часто используются для обеспечения более жесткого управления потоков данных.

Многие поставщики распространяют программные средства веб-серверов, и каждая версия имеет собственную совокупность вопросов, установок и модернизаций, менеджмент которых нужно осуществлять. Часто поставщик или третья сторона распространяют предлагаемые связанные с безопасностью установки в Интернете. Они должны быть рассмотрены и оценены в соответствии с конкретными политиками, практическим приемам и потребностями определенной организации.

### D.2.2 Серверы приложений и веб-сервисы

Специализированные веб-серверы эволюционировались в серверы приложений – серверы, которые могут прогонять функциональные части приложения как многократно используемые компоненты, которые могут вызываться 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 вызов компонента через сеть как сервиса. 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 любом устройстве, даже на тех, которые не поддерживают традиционные веб-браузеры. Многие поставщики предоставляют серверы приложений, которые поддерживают веб-сервисы. Более подробную информацию о веб-сервисах и безопасности веб-сервисов можно найти 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, менеджмент которых нужно осуществлять. Часто поставщик или третья сторона распространяют для использования предлагаемой, связанной с безопасностью установки в Интернете. Они должны быть рассмотрены и оценены относительно конкретных политик, практических приемов и потребностей определенной организации.

### D.2.3 Процесс разработки прикладных программ

Многие организации приспосабливают 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, когда 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 понимать угрозы, направленные против организации. Они должны быть осведомлены о программе обеспечения информационной безопасности и о том, где они могут получить рекомендации по ходу разработки. Прочная основа в виде Политики организации, ее практические приемы и непрерывный диалог с работниками службы обеспечения информационной безопасности будут гарантировать обеспечение программными средствами эффективной и результативной информационной безопасности.

В разработке прикладных программ, включающей требования безопасности, необходимо учитывать два аспекта. Первый заключается в том, что сам процесс разработки программных средств состоит из хорошо структурированных и хорошо документированных шагов. Целью являются создание программных средств, отвечающих исключительно своим требованиям и не по-

зволяющие случайно или преднамеренно выполнять нежелательные операции. Для достижения этой цели организация должна следовать стандарту ИСО/МЭК 21827 [13]. Дополнительную информацию о модели развития функциональных возможностей можно получить на сайте http://www.sei.cmu.edu/cmmi/. Прикладные программы с критически важными требованиями информационной безопасности должны разрабатываться, используя процессы, определяемые 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, стандартизирован и включен в стандартный процесс создания программного обеспечения для организации. Во всех проектах используется одобренная, специально приспособленная версия стандартного процесса создания программного обеспечения организации для разработки и поддержки программных средств.

Вторым аспектом является обеспечение включения 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 того, что требования полностью отвечают политике безопасности и любому регулирующему законодательству.

Поскольку знание того, как работают программные средства защиты данных, может подвергнуть риску приложение, документация, такая как результаты тестирования и инструкции для оператора, должна находиться под контролем, чтобы она неумышленно не стала доступной для несанкционированных лиц. Полное описание основных вопросов разработки можно найти в общедоступной публикации NIST SP800-64 "Соображения безопасности в жизненном цикле развития системы" на сайте http://csrc.nist.gov/publications/nistpubs/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 пункте D.2.3, пригодны для процесса приобретения, но существуют два различия в процессе разработки. Первое различие заключается в том, что процесс разработки ограничивается письменным договором. Внесение изменений в требования изменят договор и, вероятно, приведут к росту стоимости и удлинению графика. Второе отличие состоит в том, что подрядчик обычно не осведомлен о структуре и культуре труда организации. Различные предположения и неправильное представление об организации аналогичным образом будут способствовать изменениям договора. Таким образом, приобретающая организация должна быть крайне скрупулезной 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 ограниченностей 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, чтобы они не делали недействительными или не компрометировали существующие процедуры безопасности. Обычно используемым эталоном для программных средств защиты данных являются Общие Критерии (ОК), 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 http://niap.nist.gov/cc-scheme /index.html.

## D.3 Сети

### D.3.1 Глобальные сети

#### D.3.1.1 Обзор

Глобальные сети (WAN) охватывают широкие географические 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 который имеет собственный набор маршрутизаторов, коммутаторов и шлюзов с другими глобальными сетями. Так называемая обычная телефонная сеть (POTS) – это еще одна глобальная сеть. Во всех случаях глобальные сети делают возможным перемещение потока данных повсюду. Кроме того, они предоставляют множество точек доступа, где информация является уязвимой.

В организации, особенно в более крупных организациях с географическим разбросом, сеть включает соединения с глобальной сетью, такой как Интернет, несколькими локальными сетями в каждом комплексе зданий или внутри здания и несколько специальных соединений с глобальной сетью, выделенных для организации. Обычно эти выделенные соединения с глобальной сетью считаются внутренние для организации и на них нет граничных средств управления, используемых для соединения с другими фирмами или внешними глобальными сетями, подобными Интернету. Как часть регулярных оценок риска организации должны рассмотреть возможность того, что специализированные соединения с глобальной сетью могут контролироваться и, что особо ценная информация должна шифроваться. Кроме того, доступ, предоставляемый пользователям вне сети организации, должен тщательно контролироваться.

#### 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 защищаются физически, размещаясь внутри стен, шкафов и подвалов, куда имеют доступ немногие люди. Эти формы физической защиты и, возможно, периодическая проверка соединений являются единственными мерами безопасности, связанными с большинством проводных глобальных сетей. В тех случаях, когда компания приобретает специализированные линии, может проводиться определенное тестирование, но существует немного альтернатив основанному на договоре доверию к провайдеру телекоммуникационных услуг. Иногда, даже предположительно проводное соединение с глобальной сетью фактически включает линии СВЧ-связи, лазерные линии или радиочастотные линии (включая спутник), которые вводят дополнительные возможности для мониторинга информации, проходящей через глобальную сеть.

#### 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 довольно медленнодействующими (около 20 кбит/сек), существует перспектива будущих возможностей передач мегабитных 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 аналогичных возможностей 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 – смотри пункт 9.3.2.2.

### D.3.2 Локальные сети

#### D.3.2.1 Обзор

На территории комплекса зданий, или на этаже здания, или даже в главном офисе получают распространение также и локальные сети. Эти сети часто используют такие же протоколы и системы маршрутизации, как их более крупные "родственники" – глобальные сети, но обычно

обеспечивают защиту, используя некоторый вид шлюзов между локальной сетью и глобальной сетью. Шлюз может быть простым агрегатором пропускной способности и маршрутизации трафика или может включать в себя межсетевые экраны, системы поиска вирусов, обнаружения вторжения и другие граничные меры управления безопасностью (как определено в пункте 11.5). Во всех случаях поддержка понимания важности сетевых соединений и контроля за шлюзами является решающим аспектом обеспечения безопасности локальной сети. Другие особенности обсуждаются ниже.

#### D.3.2.2 Системы проводных локальных сетей

Проводные локальные сети обычно защищаются физическим образом 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 столь строгий менеджмент сети может показаться очень трудным и бесполезным пользователям предприятия.

#### 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 вопросы 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 – WEP) стали доступны открытые, совместимые и безопасные стандарты для 802.11x систем. Сделанный по образцу частного стандарта безопасности Cisco, носящего название Упрощенная расширяемая агентная платформа (LEAP), открытый стандарт, Защищенный расширяемый протокол аутентификации или PEAP стал доступен в различных беспроводных системах. При создании любой беспроводной локальной сети на предприятии необходимо тщательно рассмотреть использование PEAP или сходных механизмов обеспечения безопасности .

При создании беспроводной среды существуют две основные альтернативы архитектуры. Одна альтернатива состоит в использовании PEAP и обеспечении беспроводного доступа к сети только санкционированным системам и пользователям сети, и создании локальной сети внутри сети предприятия, рассматривая всех беспроводных пользователей как доверенных членов компании. Другой альтернативой является подсоединение беспроводной локальной сети, являющейся внешней для сети компании и использовать виртуальную частную сеть, веб-сайты SSL или аналогичные перекрытия безопасности для защиты доступа к ресурсам компании. Это более подробно объясняется в пунктах D.3.2.3.2 – D.3.2.3.4.

##### D.3.2.3.2 Беспроводная локальная сеть в границах предприятия

Компании, использующие PEAP, могут обеспечивать доступ только санкционированных пользователей беспроводной локальной сети и использование ресурсов компании. Этот вид решения все еще подвержен атакам отказа в обслуживании, но, если менеджмент и поддержка беспроводного обслуживания в основном осуществляется внутри здания или комплекса зданий, находящихся под контролем компании, этот вид решения является очень разумным. Оно предусматривает мобильных пользователей в рамках компании – ситуация, типичным примером которой служат лица, посещающие различные совещания в разных конференц-залах, или должностные лица, часто разъезжающих между различными филиалами компании. Кроме того, этот вид решения ограничивает доступ к пропускной способности сети, Интернет-соединениям и другим ресурсам компании только этими санкционированными пользователями. Существует слишком много деталей безопасной реализации PEAP в этой внутренней модели архитектуры, чтобы подробно обсуждать их здесь. Имеются много ресурсов от поставщиков и Интернета.

#### D.3.2.3.3 Беспроводная локальная сеть вне границ предприятия

Альтернативой ограничения использования беспроводной сети санкционированными пользователями является предоставление беспроводного соединения с Интернет-связью, являющегося внешним для сетей предприятия. В этом случае беспроводным пользователем может быть любой человек или любой, кто абонировал услуги. Они не будут иметь немедленный доступ к ресурсам компании. Вместо этого пользователи, которым нужен доступ к ресурсам компании, будут использовать виртуальную частную сеть (смотри пункт 11.2.1) для безопасного соединения с сетью компании.

Этому решению присущи недостатки сетевого менеджмента; однако, для пользователей могут быть преимущества. Хотя финансовые учреждения обычно не хотят, чтобы посторонние пользователи использовали ресурсы беспроводной локальной сети, например, университет может захотеть сделать беспроводную локальную сеть доступной для посетителей университетского городка. Альтернативным образом, компания управления недвижимым имуществом может захотеть сделать беспроводную локальную сеть доступной для всех арендаторов в строительном комплексе.

#### D.3.2.3.4 Другие соображения относительно беспроводной локальной сети

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

Пользователи портативных компьютеров с соединениями с беспроводной локальной сетью предъявляют дополнительные требования. Независимо от того, является ли беспроводная локальная сеть компании внутренней или внешней по отношению к сети предприятия, этим мобильным пользователям нужен доступ к ресурсам компании через виртуальную частную сеть (либо IPSEC, либо SSL) из-за 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 переезжающим руководителям с беспроводным доступом требуется Интернет связность всегда и везде. Виртуальная частная сеть предоставляет мобильному пользователю доступ к ресурсам компании, когда он находится в пути.

Основной проблемой обслуживания этих мобильных пользователей в "горячих точках" является доверие обычным Интернетовским IP-адресам. Многие компании используют внутренним образом 10. и 168. диапазоны IP-адресов для файловых услуг и услуг печати, коллективно используемых компанией. Эти немаршрутизируемые адреса часто используются повторно, так что домашняя сеть, сеть в кафетерии и сети во многих компаниях все 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 принимают решения о шифровании и маршрутизации на основе адреса, эти адреса "10." и "168." могут вызывать неоправданное доверие портативного компьютера, создавая новые потенциальные риски. Подобно виртуальной частной сети, межсетевые экраны и системы обнаружения вторжения тоже принимают решения о соединении и доверии на основе адресов. Поэтому, хотя для портативного компьютера может быть уместно доверие к принтеру на работе и даже к принтеру дома, доверие файловому серверу в кафетерии должно быть совершенно иным. Политики, программные средства и другие контрмеры в отношении этих проблем должны оцениваться и применяться на основе общей политики компании.

### D.3.3 Другие соображения, связанные с телекоммуникациями

Всегда существуют другие соображения, связанные с телекоммуникациями. Хотя реально оно только начинает набирать обороты, продолжающееся сближение речи и данных в одних и тех же сетях открывает новый ряд проблем телекоммуникаций и контрмер. Недавно решения в форме речевых межсетевых экранов, магистральных виртуальных частных сетей и мультимедийных

систем обнаружения вторжения, которые рассматривают проблемы слияния данных/речи, начали вырисовываться как продукция и серьезно рассматриваются крупными поставщиками. Эти решения также реализуются компаниями, часто окупаясь экономией затрат в результате более хорошего управления речевыми телекоммуникациями в рамках компании.

## Библиография


[1] ITU-T Recommendation X.509 (2001) | ISO/IEC 9594-8, Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks — Part 8

| | |
|---|---|
| [2] Международный стандарт ИСО 7498-2 | Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture |
| [3] Международный стандарт ISO/IEC 10181-1 | Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview |
| [4] Международный стандарт ИСО/МЭК 13335 (все части) | Информационная технология – Руководящие указания по управлению защитой информационных технологий Information technology — Security techniques — Management of information and communications technology security |
| [5] Международный стандарт ИСО 13491-1 | Banking — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods |
| [6] Международный стандарт ИСО/МЭК 13888 | Information Technology — Security Techniques — Non-Repudiation |
| [7] Международный стандарт ИСО/МЭК 15408 | Information Technology — Security Techniques — Evaluation criteria for IT security |
| [8] Международный стандарт ИСО/МЭК 18043 | Information technology — Deployment and operation of Intrusion Detection Systems |
| [9] Технический отчет ИСО/МЭК 18044 | Информационная технология – Методы и средства обеспечения безопасности – Менеджмент инцидентов информационной безопасности<br>Information technology — Security techniques — Management of information and communications technology security |
| [10] Технический отчет ИСО/МЭК 19038 | Banking and related financial services — Triple DEA — Modes of operation — Implementation guidelines |
| [11] Международный стандарт ИСО 19092 | Financial Services — Biometrics |
| [12] Международный стандарт ИСО/МЭК 19790 | Information technology — Security techniques — Security requirements for cryptographic modules |

[13] Международный стандарт ИСО/МЭК 21827 — Information Technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM®)

[14] ANSI X9.52-1998, Triple Data Encryption Algorithm Modes of Operation

[15] ANSI X9.79-2001, Financial Services Public Key Infrastructure (PKI) Policy and Practices Framework

[16] ANSI X9.84-2003, Biometric Information Management and Security for the Financial Services Industry

[17] FIPS 140-2, Security Requirements for Cryptographic Modules, National Institute for Standards and Technology (USA.). http://csrc.nist.gov/cryptval/140-2.htm

[18] FIPS 197, Advanced Encryption Standard (AES), National Institute for Standards and Technology (USA.). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[19] Security Of Electronic Money, published by the Bank of International Settlement, Basle, August 1996

[20] W3C Extensible Markup Language (XML) 1.0 (Second Edition), W3C Recommendation, Copyright © [6 October 2000] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2000/REC-xml-20001006/

[21] Institute of Internal Auditors Standards for the Professional Practice of Internal Auditing

[22] Gramm-Leach-Bliley (GLB) Act of 1999, http://www.senate.gov/~banking/conf/