ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

МЕТОДЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ СВОД ПРАВИЛ ПО УПРАВЛЕНИЮ ЗАЩИТОЙ ИНФОРМАЦИИ

Information Technology
SECURITY TECHNIQUES
CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT

СТ РК ИСО/МЭК 17799-2006
(ISO/IEC 17799-2005, IDT)

Издание официальное

Комитет по техническому регулированию и метрологии
Министерства индустрии и торговли Республики Казахстан
(Госстандарт)

Астана

Предисловие

1 ПОДГОТОВЛЕН И ВНЕСЕН ТОО «Специальное конструкторско-технологическое бюро «Гранит» на основе собственного аутентичного перевода стандарта, указанного в пункте 3

2 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ приказом Комитета по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан от 15 декабря 2006 г. № 550

3 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 17799-2005 «Технологии информационные. Методы обеспечения защиты. Кодекс установившейся практики по управлению безопасностью информации» (ISO/IEC 17799-2005 «Information technology. Security techniques. Code of practice for information security management»)

4 В настоящем стандарте реализованы нормы законов Республики Казахстан О техническом регулировании, О языках в Республике Казахстан, Соглашения Всемирной торговой организации по техническим барьерам в торговле

5 СРОК ПЕРВОЙ ПРОВЕРКИ 2011 год
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

6 ВВЕДЕН ВПЕРВЫЕ

Содержание

1 Область применения 1
2 Термины и определения 1
3 Структура настоящего стандарта 2
3.1 Разделы 2
3.2 Основные категории безопасности 3
4 Оценка и обработка риска 3
4.1 Процесс оценки рисков 3
4.2 Процесс обработки рисков 4
5 Политика безопасности 5
5.1 Политика информационной безопасности 5
6.Организация информационной безопасности 6
6.1 Внутренняя организация 6
6.2 Обеспечение безопасности при наличии доступа к информационным системам сторонних организаций 12
7 Управление активами 17
7.1 Ответственность за активы 17
7.2 Классификация информации 19
8 Вопросы безопасности, связанные с кадровыми ресурсами 20
8.1 Перед трудоустройством 20
8.2 Во время работы по трудовому соглашению 23
8.3 Прекращение действия трудового соглашения или его изменение 25
9 Физическая защита и защита от воздействий окружающей среды 27
9.1 Охраняемые зоны 27
9.2 Безопасность оборудования 30
10 Управление средствами связи и операциями 34
10.1 Процедуры эксплуатации и обязанности 34
10.2 Управление поставкой услуг третьей стороной 37
10.3 Планирование нагрузки и приемка систем 39
10.4 Защита от вредоносного и подвижного кода 40
10.5 Дублирование 43
10.6 Управление безопасностью сетей 44
10.7 Манипулирование носителями информации 45
10.8 Обмен информацией 47
10.9 Сервисы электронной торговли 52
10.10 Мониторинг 54
11 Контроль доступа 58
11.1 Требование бизнеса по обеспечению контроля доступа 58
11.2 Управление доступом пользователя 59
11.3 Обязанности пользователя 62
11.4 Контроль сетевого доступа 64
11.5 Контроль доступа к операционной системе 68
11.6 Контроль доступа к приложениям и информации 72
11.7 Мобильные вычислительные устройства и удалённый доступ 74
12 Приобретение, усовершенствование и обслуживание информационных систем 76
12.1 Требования безопасности информационных систем 76
12.2 Правильная обработка приложений 77
12.3 Криптографические средства контроля 80
12.4 Безопасность системных файлов 83

12.5 Безопасность в процессах разработки и поддержки 85
12.6 Управление техническими уязвимостями 88
13 Управление инцидентами нарушения информационной безопасности 90
13.1 Сообщение о нарушениях и слабых местах информационной безопасности 90
13.2 Управление инцидентами нарушения информационной безопасности и их усовершенствование 92
14.Управление непрерывностью бизнеса 95
14.1 Аспекты информационной безопасности управления непрерывностью бизнеса 95
15 Соответствие требованиям 100
15.1 Соответствие правовым требованиям 100
15.2 Соответствие политикам и стандартам безопасности, и техническое соответствие 104
15.3 Вопросы для рассмотрения при аудите информационных систем 105
Приложение (справочное) Библиография 107

Введение

Информация является активом, который, подобно другим важным деловым активам, имеет большое значение для бизнеса организации и, следовательно, должен быть адекватно защищён. Это особенно важно в условиях растущей взаимосвязанности деловой среды. В результате этого усиления взаимосвязанности в настоящее время информация подвергается всё большему числу и разнообразию угроз и уязвимостей (см. Руководство Организации по экономическому сотрудничеству и развитию по безопасности информационных систем и сетей [1]).

Информация может существовать в различных видах. Она может быть напечатана или написана на бумаге, храниться в электронном виде, передаваться по почте или электронными средствами, отображаться на плёнке или выдаваться в разговоре. Какую бы форму ни принимала информация или средства, которыми она передаётся или на которых она хранится, она всегда должна быть соответствующим образом защищена.

Информационная безопасность есть защита информации от множества угроз для обеспечения непрерывности делового процесса, минимизации делового риска и максимальной прибыли от инвестированного капитала и возможностей деловой деятельности.

Информационная безопасность достигается посредством реализации соответствующего набора мер контроля, включая политики, процедуры, процессы, организационные структуры и функции программного и аппаратного обеспечения. Эти меры контроля должны быть определены, реализованы, проверены, пересмотрены и, при необходимости, улучшены для соответствия специфическим целям обеспечения безопасности и деловой деятельности. Это должно осуществляться совместно с другими процессами управления деловой деятельностью.

Информация и процессы, системы и сети её обеспечения являются важными корпоративными активами. Определение, достижение, поддержание и повышение информационной безопасности могут быть весьма существенными для поддержания конкурентного преимущества движения денежной наличности, рентабельности, соблюдения правовых норм и коммерческого престижа.

Организации и их информационные системы и сети сталкиваются с угрозой безопасности от множества источников, включая мошенничество с помощью компьютера, шпионаж, саботаж, вандализм, пожар или наводнения. Причины ущерба, такие как злоумышленный код, компьютерное хакерство и атаки «отказ в обслуживании» стали более распространёнными, амбициозными и сложными.

Информационная безопасность важна для деловой деятельности, как в общественном, так и в частном секторе в смысле защиты критичных инфраструктур. В обоих секторах информационная безопасность функционирует как нечто, дающее возможность что-либо сделать, например, для получения электронной формы правления или электронного бизнеса, а также для избежания или снижения соответствующих рисков. Взаимосвязь между общественными и частными сетями и совместное использование информационных ресурсов повышают трудность в установлении контроля доступа. Тенденция к использованию распределённой обработки данных также понижает эффективность центрального контроля специалистами.

Многие информационные системы незащищены конструктивно. Безопасность, которая может быть установлена техническими средствами, ограничена и должна поддерживаться соответствующим менеджментом и процедурами. Для определения необходимых мер контроля требуется тщательное планирование и внимание к деталям. Управление информационной безопасностью требует, как минимум, участия всех работников организации. Для этого также может потребоваться участие акционеров, поставщиков, третьих

сторон, заказчиков и других внешних сторон. Может также потребоваться консультация специалиста из посторонних организаций.

Важно, чтобы организация определила свои требования безопасности. Существуют три основных источника требований безопасности:

1 Один источник выведен из оценки рисков для организации с учётом общей стратегии и целей деловой деятельности организации. Посредством оценки риска определяются угрозы для активов, оцениваются уязвимость и вероятность появления этих угроз, и их потенциальное воздействие.

2 Другим источником являются юридические, нормативные, регулятивные и договорные требования, которым должны удовлетворять организация, её торговые партнёры, подрядчики и поставщики услуг, а также их социально-культурная среда.

3 Дальнейшим источником является определённый набор принципов, целей и бизнес-требований для обработки информации, которые организация разработала для поддержки своих операций.

Требования безопасности определяются посредством методической оценки рисков безопасности. Расходы на меры контроля необходимо сбалансировать с ущербом для деловой деятельности, который может быть результатом сбоев в системе безопасности.

Результаты оценки рисков помогут направлять и определять соответствующие действия и приоритеты руководства по менеджменту рисков информационной безопасности, а также для реализации мер контроля, выбранных для защиты от этих рисков.

Оценка риска должна периодически повторяться, чтобы реагировать на любые изменения, которые могут повлиять на результаты оценки риска.

Дополнительную информацию об оценке рисков безопасности можно найти в 4.1 «Оценка рисков безопасности».

После определения требований и рисков безопасности и принятия решений об обработке рисков необходимо выбрать и реализовать меры контроля, которые обеспечивали бы снижение рисков до приемлемого уровня. Меры контроля можно выбирать из этого стандарта или из других наборов мер контроля, а также можно создать при необходимости новые меры для удовлетворения каких-то специфических потребностей. Выбор мер контроля безопасности зависит от организационных решений, основанных на критериях принятия рисков, вариантах обработки рисков и общего подхода к менеджменту риска, принятых в организации, а также быть предметом для соответствующих национального и международного законодательства и правовых положений.

Некоторые меры контроля в данном стандарте могут рассматриваться как руководящие принципы для управления информационной безопасностью и являются приемлемыми для многих организаций. Ниже они подробно разъясняются в разделе под заголовком «Отправная точка информационной безопасности».

Дополнительную информацию о выборе мер контроля и других вариантов обработки риска можно найти в 4.2 «Процесс обработки риска».

Некоторые меры контроля можно рассматривать как хорошую отправную точку для реализации информационной безопасности. Они основаны на законодательных требованиях или считаются установившейся практикой для информационной безопасности.

Меры контроля, считающиеся необходимыми для организации с точки зрения законодательства, включают в зависимости от применяемого законодательства следующее:

a) защиту данных и неприкосновенность личной информации (см. 15.1.4);

b) защиту документов (см. 15.1.3);

c) права на интеллектуальную собственность (см. 15.1.2).

Меры контроля, считающиеся общепринятой практикой для информационной безопасности, включают:

a) документ политики информационной безопасности (см. 5.1.1);

b) распределение обязанностей по обеспечению информационной безопасности (см. 6.1.3);
c) обучение, подготовку и осведомлённость по информационной безопасности (см. 8.2.2);
d) правильную обработку в приложениях (см. 12.2);
e) управление технической уязвимостью (см. 12.6);
f) управление непрерывностью деловой деятельности (см. раздел 14);
g) управление инцидентами и усовершенствованиями информационной безопасности (см. 13.2).

Эти меры контроля применимы для большинства организаций и в большинстве сред.

Необходимо отметить, что хотя все меры контроля в этом стандарте важны и должны учитываться, действенность любой меры контроля в свете специфических рисков, имеющихся у организации. Следовательно, хотя вышеуказанный подход считается хорошей отправной точкой, он не подменяет выбор мер контроля, основанный на оценке риска.

Опыт показал, что для успешной реализации информационной безопасности внутри организации часто бывают критическими следующие факторы:

a) цели и политика информационной безопасности, а также действия, отражающие цели деловой деятельности;
b) подход и основа для реализации поддержания мониторинга и усовершенствования информационной безопасности, которые совместимы с культурой организации;
c) видимая поддержка и приверженность от всех слоёв руководства;
d) хорошее понимание требований информационной безопасности, оценки риска и менеджмента риска;
e) эффективный маркетинг информационной безопасности для всех менеджеров, сотрудников и других сторон для обеспечения осведомлённости;
f) распределение руководства по политике и стандартам информационной безопасности среди всех менеджеров, сотрудников и других сторон;
g) обязательство по финансированию деятельности по управлению информационной безопасностью;
h) обеспечение соответствующей осведомлённости, подготовки и обучения;
i) установление эффективного процесса руководства инцидентами информационной безопасности;
j) реализация системы измерения, которая используется для оценки характеристик управления информационной безопасностью, и предложения обратной связи по его улучшению.

Примечание - Измерения информационной безопасности находятся вне области действия этого стандарта.

Данное практическое правило может рассматриваться как исходная точка для разработки специфических руководств организации. Не все меры контроля в этом правиле могут быть применимы. Более того, могут потребоваться дополнительные меры контроля и руководства, не включённые в этот стандарт. После разработки документов, содержащих дополнительные руководства или меры контроля, может быть полезно, включить перекрёстные ссылки в параграфы этого стандарта, где это допустимо, для облегчения проверки на соответствие аудиторами и партнёрами по деловой деятельности.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология
МЕТОДЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ
СВОД ПРАВИЛ ПО УПРАВЛЕНИЮ ЗАЩИТОЙ ИНФОРМАЦИИ

Information technology. Security techniques. Code of practice for information security management

Дата введения 2008.01.01.

1 Область применения

Настоящий государственный стандарт устанавливает основные руководящие принципы для инициирования, реализации, поддержки и усовершенствования руководства информационной безопасностью в организации. Цели, приведённые в этом стандарте, обеспечивают общее руководство по решению общепринятых задач управления информационной безопасностью.

Цели и меры контроля настоящего стандарта предназначены для реализации с целью соответствия требованиям, идентифицированным оценкой риска. Настоящий стандарт может служить практическим руководством по разработке организационных стандартов безопасности и эффективных правил управления безопасностью.

2 Термины и определения

Последующие термины и определения приводятся с целью облегчения прочтения данного документа:

2.1 **Активы** (asset): Всё, что имеет ценность для организации [2].

2.2 **Мера контроля** (control): Средства управления рисками, включая политики, процедуры, руководства, правила или организационные структуры, которые могут быть административного, технического, управленческого или юридического характера.

Примечание - Мера контроля может также использоваться как синоним слов «меры безопасности» и «контрмера».

2.3 **Рекомендации** (guidelines): Описание, которое разъясняет, что и как должно быть сделано для достижения установленных целей [2].

2.4 **Средства обработки информации** (information processing facilities): Любая система обработки информации, служба или инфраструктура или физические месторасположения, в которых они размещены.

2.5 **Безопасность информации** (information security): Сохранение конфиденциальности, целостности и доступности информации, кроме того, сюда можно включить другие свойства, такие как аутентичность, подотчётность, неоспоримость и надёжность.

2.6 **Событие информационной безопасности** (information security event): Событием информационной безопасности является идентифицированное возникновение состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности, отказ средств защиты или ранее неизвестную ситуацию, которая может быть связана с безопасностью[3].

Издание официальное

2.7 **Инцидент с информационной безопасностью** (information security incident): На инцидент с информационной безопасностью указывают отдельное или серия нежелательных или неожиданных событий информационной безопасности, обладающие существенной вероятностью подвергания опасности деловых операций или создания угрозы информационной безопасности [3].

2.8 **Политика** (policy): Общее намерение и направление, формально выраженные руководством.

2.9 **Риск** (risk): Комбинация вероятности события и его последствий [4].

2.10 **Анализ риска** (risk analysis): Систематическое использование информации для идентификации источников риска и оценки степени риска [4].

2.11 **Оценка риска** (risk assessment): Общий процесс анализа риска и оценка степени риска [4].

2.12 **Оценивание риска** (risk evaluation): Процесс сравнения оцененного риска с данными критериями риска с целью определения значимости риска [4].

2.13 **Менеджмент риска** (risk management): Скоординированные действия по руководству и управлению организацией в отношении риска [4].

Примечание - Обычно менеджмент риска включает в себя оценку риска, обработку риска, принятие риска и коммуникация риска.

2.14 **Обработка риска** (risk treatment): Процесс выбора и реализации мер по модификации риска [4].

2.15 **Третья сторона** (third party): Лицо или организация, признанные независимыми от заинтересованных сторон по отношению к рассматриваемому вопросу [5].

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

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

3 Структура настоящего стандарта

В стандарте содержатся 11 разделов по мерам контроля безопасности, совместно включающих 39 основных категорий безопасности и один вводный раздел, знакомящий с оценкой и обработкой рисков.

3.1 Разделы

В каждом разделе содержится некоторое число основных категорий безопасности. В одиннадцати разделах (вместе с основными категориями безопасности, включёнными в каждый раздел) описываются:

a) политика безопасности (1);
b) организация информационной безопасности (2);
c) управление активами (2);
d) безопасность кадровых ресурсов (3);
e) физическая и экологическая безопасность (2);
f) управление средствами связи и операциями (10);
g) контроль доступа (7);
h) приобретение, разработка и обслуживание информационных систем (6);
i) управление инцидентами с информационной безопасностью (2);
j) управление непрерывностью бизнес-процесса (1);
k) соответствие (3).
l)

Примечание - Порядок разделов в данном стандарте не подразумевает степень их значимости. В зависимости от обстоятельств все разделы могут быть значимыми, следовательно, каждая организация, применяющая этот стандарт, должна определять применимые ей разделы и степень их важности для отдельных бизнес-процессов. Также, все перечни в этом стандарте не имеют приоритета, если это не отмечено заранее.

3.2 Основные категории безопасности

В каждой основной категории безопасности содержится:

a) цель контроля, формулирующая то, что должно быть достигнуто; и

b) одно или несколько мер контроля, которые можно применить для достижения цели контроля.

Описания контроля сконструированы следующим образом:

Определение

Определяет специфический управляющий оператор для достижения цели контроля.

Руководство по реализации

Обеспечивает более подробную информацию для поддержки реализации контроля и соответствия цели контроля.

Некоторая часть этого руководства может быть неподходящей для всех случаев и можно найти несколько более пригодных путей реализации контроля.

Дополнительная информация

Обеспечивает дальнейшую информацию, которая может потребоваться для рассмотрения, например, юридические соображения и ссылки на другие стандарты.

4 Оценка и обработка риска

4.1 Процесс оценки рисков

Оценки рисков должны идентифицировать, определять количество рисков и их приоритеты по отношению к критериям принятия рисков и целям, подходящим организации. Результаты должны направлять и определять соответствующие действия руководства и приоритеты для управления рисками безопасности и для реализации мер контроля, выбранных для защиты от таких рисков. Может потребоваться неоднократное повторение процесса оценки рисков и выбора мер контроля, чтобы охватить различные подразделения организации или отдельные информационные системы.

Оценка риска должна включать систематический подход определения величины рисков (анализ рисков) и процесс сравнения оценённых рисков с критериями рисков с целью определения значимости рисков (оценка степени рисков).

Оценки рисков должны также проводиться периодически для реагирования на изменения в требованиях безопасности и в ситуации рисков, например, в активах, угрозах, уязвимостях, воздействиях, оценке степени рисков и при возникновении значительных изменений. В целях получения сравнимых и воспроизводимых результатов эти оценки рисков должны предприниматься методическим образом.

Чтобы быть эффективной, оценка рисков безопасности информации должна иметь чётко определённую область действия и включать взаимосвязь с оценками рисков в других областях, если это целесообразно.

Областью действия оценки риска могут быть или вся организация, подразделения организации, отдельная информационная система, специфические компоненты системы, или службы, где она осуществима, реалистична и полезна. Примеры методологий оценки риска рассматриваются в [6].

4.2 Процесс обработки рисков

Перед рассмотрением проблемы обработки рисков организация должна определить критерии определения принятия или неприятия рисков. Риски могут приниматься, если, например, сделана оценка, что риск незначителен или что стоимость обработки нерентабельна для организации. Подобные решения должны регистрироваться.

Для каждого из идентифицированных рисков, следующих за оценкой рисков, необходимо принимать решение по обработке риска. Возможными вариантами для обработки риска включают:

a) применение подходящих мер контроля для уменьшения рисков;
b) сознательное и объективное принятие рисков при условии, что они соответствуют политике организации и критериям принятия рисков;
c) избежание рисков путём недопущения действий, вызывающих возникновение рисков;
d) передачу ассоциированных рисков другим сторонам, например, страховщикам или поставщикам.

Для рисков, где решение по обработке рисков принималось относительно соответствующих мер контроля, эти меры контроля должны выбираться и реализовываться для удовлетворения требований, идентифицированных оценкой рисков. Меры контроля должны обеспечивать снижение рисков до приемлемого уровня, учитывая:

a) требования и ограничения национальных и международных законодательств и положений;
b) организационные цели;
c) эксплуатационные требования и ограничения;
d) затраты на реализацию и эксплуатацию относительно снижаемых рисков и соответствия оставшихся рисков требованиям и ограничениям организации;
e) необходимость сопоставления вложений в реализацию и эксплуатацию мер контроля с вероятным ущербом как следствием отказа в обеспечении в обеспечении безопасности.

Меры контроля могут выбираться из этого стандарта или других наборов мер контроля, а для удовлетворения специфических потребностей организации могут создаваться новые мер контроля. Надо признать, что некоторые меры контроля могут не подходить к каждой информационной системе или среде и могут быть невыполнимы для всех организаций. В качестве примера в 10.1.3 способ разделения обязанностей для предотвращения мошенничества или ошибок. Для небольших организаций разделение всех обязанностей может быть невозможным, и могут потребоваться другие пути достижения той же цели контроля. Как другой пример, в 10.10 описывается способ мониторинга использования системы и сбора свидетельств. Описанные меры контроля, например, регистрация событий, могут вступать в конфликт с существующим законодательством относительно защиты частной жизни заказчиков или на рабочем месте.

Меры контроля информационной безопасности должны рассматриваться на стадии создания спецификаций и требований для систем и проектов. Неспособность осуществления этого может привести к дополнительным расходам, принятию менее эффективных решений, и, в худшем случае, к неспособности обеспечения адекватной безопасности.

Необходимо помнить, что ни один набор мер контроля не может обеспечить полную безопасность, и для поддержки целей организации, а также в целях контроля, оценки и повышения эффективности и результативности мер контроля безопасности необходимо реализовать дополнительные действия по управлению.

5 Политика безопасности

5.1 Политика информационной безопасности

Цель: обеспечить поддержку и вовлечение высшего руководства в решение вопросов, связанных с информационной безопасностью в соответствии с бизнес-требованиями и подходящими законами и положениями.

Руководство должно выработать четкую позицию в соответствии с бизнес целями и демонстрировать поддержку и заинтересованность в отношении обеспечения информационной безопасности посредством разработки и поддержки политики информационной безопасности в рамках всей организации.

5.1.1 Документальное оформление

Определение

Политика информационной безопасности должна быть утверждена высшим руководством, издана и доведена до сведения всех сотрудников и соответствующих внешних сторон.

Руководство по реализации

Документ о политике информационной безопасности должен устанавливать ответственность руководства и излагать подход организации к управлению информационной безопасностью. Политика должна содержать следующие положения:

a) определение информационной безопасности, ее общих целей и сферы действия, а также упоминание значения безопасности как инструмента, обеспечивающего возможность совместного использования информации (см. Введение);
b) изложение намерений руководства, поддерживающих цели и принципы информационной безопасности в соответствии со стратегией и целями бизнеса;
c) основание для установки целей контроля и мер контроля, включая структуру оценки риска и менеджмент риска;
d) краткое изложение наиболее существенных для организации политик безопасности, принципов, стандартов и требований, включающее:
   1) соответствие законодательным, регулятивным требованиям и договорным обязательствам;
   2) требования в отношении обучения и осведомлённости в вопросах безопасности;
   3) управление непрерывностью бизнеса;
   4) ответственность за нарушения политики информационной безопасности;
e) определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности;
f) ссылки на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры безопасности для определенных информационных систем, а также правила безопасности, которым должны следовать пользователи.

Такая политика информационной безопасности должна быть доведена до сведения пользователей в рамках всей организации в уместной, доступной и понятной форме.

Дополнительная информация

Политика информационной безопасности может быть частью документа общей политики. Если политика информационной безопасности распространяется вне организации, то нужно обратить внимание на неразглашение секретной информации. Дополнительную информацию можно найти в [2].

5.1.2 Пересмотр политики информационной безопасности

Определение

Политика информационной безопасности должна пересматриваться через запланированные промежутки времени или в случае появления существенных изменений в целях обеспечения её непрерывной стабильности, адекватности и эффективности.

Руководство по реализации

Политика информационной безопасности должна иметь владельца, который утвердил административную ответственность за развитие, пересмотр и оценку политики безопасности. Пересмотр должен включать возможности оценки для улучшения политики информационной безопасности организации и подход к управлению информационной безопасностью в ответ на изменения в организационной среде, деловой ситуации, юридических условиях или технической среде.

При пересмотре политики информационной безопасности необходимо учитывать результаты пересмотров управления. Здесь должны быть определены процедуры пересмотра, включая график или продолжительности пересмотра.

Входные данные для пересмотра управления должны включать информацию по:

a) обратной связи от заинтересованных сторон;
b) результатам независимых пересмотров (см.6.1.8);
c) статусу превентивных и корректирующих действий (см.6.1.8 и 15.2.1);
d) результатам предыдущих пересмотров;
e) характеристикам процесса и соответствию политики безопасности информации;
f) изменениям, которые могут повлиять на подход организации к управлению информационной безопасностью, включая изменения в организационной среде, деловой ситуации, наличии ресурсов, договорных, регулятивных или юридических условиях или в технической среде;
g) тенденции, связанные с угрозами и уязвимостями;
h) сообщённым инцидентам с информационной безопасностью (см.13.1);
i) рекомендациям, представленным соответствующими учреждениями (см.6.1.6).

Выходные данные из пересмотра управления должны включать любые решения и действия, связанные с:

a) усовершенствованием подхода организации к управлению информационной безопасностью и его процессами;
b) усовершенствованием целей и мер контроля;
c) улучшением распределения ресурсов и/или обязанностей.

Пересмотр управления необходимо регистрировать.

Пересмотренная политика должна утверждаться руководством.

6 Организация информационной безопасности

6.1 Внутренняя организация

Цель: управление информационной безопасностью в организации.

Структуру управления следует создавать так, чтобы она способствовала инициации и осуществлению контроля за внедрением информационной безопасности в организации.

Высшее руководство должно утверждать политику информационной безопасности, назначать ответственных лиц в области информационной безопасности и координировать и пересматривать внедрение информационной безопасности в организации.

При необходимости следует предусмотреть наличие источника информации по во-

просам информационной безопасности внутри организации, к которому могут обращаться заинтересованные сотрудники. Следует налаживать контакты с внешними специалистами (или группами, включая соответствующие органы) по безопасности для того, чтобы быть в курсе отраслевых тенденций, стандартов и методов оценки, а также с целью адекватного реагирования на инциденты нарушения информационной безопасности. Следует поощрять многопрофильный подход к информационной безопасности.

6.1.1 Обязательства руководства по обеспечению информационной безопасности

Определение

Руководство должно активно поддерживать безопасность внутри организации посредством ясных указаний, демонстрированных обязательств, чётких постановок задач и осведомлённости об обязанностях по обеспечению информационной безопасности.

Руководство по реализации

Руководство организации должно:

a) обеспечить, чтобы цели обеспечения информационной безопасности были определены, удовлетворяли организационным требованиям и были интегрированы в соответствующие процессы;
b) формулировать, пересматривать и утверждать политику информационной безопасности;
c) пересматривать эффективность реализации политики информационной безопасности;
d) обеспечивать чёткое управление и зримую поддержку руководством инициатив в деле обеспечения безопасности;
e) предоставлять ресурсы для обеспечения информационной безопасности;
f) утверждать распределение специфических ролей и обязанностей по информационной безопасности в организации;
g) инициировать планы и программы по поддержанию осведомлённости об информационной безопасности;
h) обеспечивать координацию реализации мер контроля за информационной безопасностью в организации (см. 6.1.2).

Руководство организации должно определять потребность в консультации специалиста внутри организации или со стороны по вопросам информационной безопасности, просматривать и координировать результаты консультации по всей организации.

В зависимости от масштаба организации такие обязанности должны выполняться специальным собранием руководства или постоянным руководящим органом, таким, как совет директоров.

Дополнительная информация

Дальнейшая информация содержится в стандарте [2].

6.1.2 Координация информационной безопасности

Определение

Действия по обеспечению информационной безопасности должны координироваться представителями различных подразделений организации с соответствующими ролями и на соответствующих должностях.

Руководство по реализации

Обычно координация информационной безопасности должна включать взаимосвязь и сотрудничество менеджеров, потребителе, администраторов, разработчиков прикладных программ, аудиторов и персонала службы безопасности и квалифицированных специалистов в таких областях, как страхование, юридические вопросы, кадровые ресурсы, инфор-

мационные технологии и управление рисками.

Эта деятельность должна:

a) обеспечивать соответствие выполнения действий по обеспечению информационной безопасности политике информационной безопасности;
b) определять действия в случае несоответствия;
c) утверждать методологии и процессы обеспечения информационной безопасности, например, оценку рисков, классификацию информации;
d) идентифицировать значительные изменения угроз и подвергание информации и средств обработки информации угрозам;
e) оценивать адекватность и координировать реализацию мер контроля информационной безопасности;
f) эффективно способствовать обучению, подготовке по информационной безопасности и осведомлённости о ней;
g) оценивать информацию, полученную от мониторинга и пересмотра инцидентов информационной безопасности и рекомендовать соответствующие действия в ответ на идентифицированные инциденты информационной безопасности.

Если в организации не задействована группа перекрёстного функционирования, например, такая группа не подходит для масштабов организации, вышеописанные действия должны осуществляться другим подходящим органом управления или отдельным менеджером.

6.1.3 Распределение обязанностей по обеспечению информационной безопасности

Определение

Все обязанности по обеспечению информационной безопасности должны быть чётко определены.

Руководство по реализации

Распределение обязанностей по обеспечению информационной безопасности должно проводиться в соответствии с политикой информационной безопасности (см. раздел 4). Следует четко определить обязанности по защите отдельных активов и по выполнению конкретных процедур, связанных с информационной безопасностью. Обязанность следует дополнить, где необходимо, более детальными руководствами для конкретных областей и средств обработки информации. Должна быть четко определена конкретная ответственность в отношении защиты активов и выполнения определённых процессов, связанных с информационной безопасностью, например, таких как планирование непрерывности бизнеса.

Отдельные лица, связанные с обеспечением безопасности могут передавать свои полномочия другим лицам. Тем не менее, они остаются ответственными за обеспечение безопасности и должны определять, что любые переданные полномочия реализуются должным образом.

Границы ответственности каждого руководителя должны быть четко установлены; в частности должно иметь место следующее:

a) различные активы и процессы (процедуры) безопасности, связанные с каждой отдельной системой, должны быть выделены и ясно определены;
b) необходимо назначить ответственных за каждый актив или процедуру безопасности и детали этой ответственности должны быть документированы;
c) уровни полномочий (авторизации) должны быть ясно определены и документированы.

Дополнительная информация

Во многих организациях на руководителя службы информационной безопасности

возлагается общая ответственность за разработку и внедрение системы информационной безопасности, а также за оказание содействия в определении мероприятий по управлению информационной безопасностью.

В то же время, ответственность за выделение ресурсов и реализацию мер и средств контроля в большинстве случаях возлагается на руководителей среднего звена. Общепринятой практикой является назначение Ответственного лица (владельца) для каждого информационного актива, в чьи повседневные обязанности входит обеспечение безопасности данного актива.

6.1.4 Процесс получения разрешения на использование средств обработки информации

Определение

Необходимо определить и внедрить процесс получения разрешения на использование новых средств обработки информации.

Руководство по реализации

Следует рассмотреть следующие меры контроля процесса получения разрешения:

a) новые средства должны быть соответствующим образом одобрены со стороны руководства пользователей и администраторов средств управления, авторизующих их цель и использование. Одобрение следует также получать от менеджера, ответственного за поддержание среды безопасности локальной информационной системы, чтобы обеспечить уверенность в том, что все соответствующие политики безопасности и требования соблюдены;
b) аппаратные средства и программное обеспечение следует проверять на совместимость с другими компонентами системы;
c) использование личных или являющихся частной собственностью средств обработки информации, например: портативные компьютеры, домашние компьютеры или приборы, работающие с рук, для обработки деловой информации может внести новые уязвимости и поэтому нужно определить и внедрить необходимые меры контроля.

6.1.5 Соглашения о конфиденциальности

Определение

Требования по соглашениям о конфиденциальности или неразглашении, отражающие потребности организации по защите безопасности, должны быть определены и регулярно пересмотрены.

Руководство по реализации

Соглашения о конфиденциальности или неразглашении должны отвечать требованию защиты конфиденциальной информации при помощи имеющих правовую силу условий соглашения. Для определения требований по соглашениям о конфиденциальности или неразглашении необходимо рассмотреть следующие элементы:

a) определение информации, которая должна быть защищена (т.е. конфиденциальная информация);
b) предполагаемая продолжительности соглашения, включая случаи, когда конфиденциальность должна поддерживаться бесконечно;
c) требуемые действия по окончанию соглашения;
d) обязанности и действия подписавших сторон для избежания несанкционированного разглашения информации (такого как «принцип необходимого знания»);
e) собственность на информацию, коммерческие секреты и интеллектуальную собственность и то, как она связана с защитой конфиденциальной информации;

f) разрешённое использование конфиденциальной информации и право подписавшей стороны использовать информацию;
g) право аудита и мониторинга действий, в которых задействована конфиденциальная информация;
h) процесс уведомления и сообщения о несанкционированном разглашении или нарушении конфиденциальности информации;
i) условия о возврате или уничтожении информации при прекращении действия соглашения;
j) предполагаемые действия в случае нарушения данного соглашения.

В соглашении о конфиденциальности или неразглашении могут потребоваться другие элементы, основанные на требованиях безопасности или иной организации.
Соглашения о конфиденциальности и неразглашении должны соответствовать всем применяемым правовым нормам и правилам юрисдикции, которые применяются (см. также 15.1.1).

Требования к соглашениям о конфиденциальности и неразглашении должны пересматриваться периодически и в случае появления изменений, влияющих на эти требования.

Дополнительная информация

Соглашения о конфиденциальности и неразглашении защищают информацию организации и информируют подписавшиеся стороны об их обязанностях по защите, использовании и разглашении информации ответственным и узаконенным образом.

У организации может возникнуть необходимость использовать различные виды соглашений о конфиденциальности и неразглашении в различных обстоятельствах.

6.1.6 Контакт с властями

Определение

Необходимо поддерживать соответствующие контакты с компетентными органами.

Руководство по реализации

Организации должны иметь процедуры, обозначающие, когда и кто должен контактировать с органами (например, с полицией, пожарной службой, органами надзора), и как своевременно сообщать об обнаруженных инцидентах информационной безопасности, если есть подозрение о возможных нарушениях правовых норм.

При атаке из Интернета организациям может потребоваться, чтобы третьи стороны (например, поставщик услуг Интернета или оператор сети связи) предприняли действия против источника атаки.

Дополнительная информация

Поддержание подобных контактов может быть требованием для содействия управлению инцидентами информационной безопасности (см.13.2) или планирования чрезвычайных обстоятельств и непрерывности бизнеса (раздел 14). Контакты с регулятивными органами также полезны для предупреждения и подготовки к грядущим изменениям в правовых нормах и правилах, которые организация должна соблюдать. Контакты с другими органами должны включать службы коммунальных услуг, аварийные службы, службы охраны труда, например, пожарные службы (обеспечение непрерывности бизнеса), поставщик средств телекоммуникации (обеспечение линейной маршрутизации) и службой водоснабжения (обеспечение средств охлаждения оборудования).

6.1.7 Контакты со специальными группами (по конкретным проблемам)

Определение

Необходимо поддерживать соответствующие контакты со специальными группами, конференциями (форумами) специалистов по безопасности и профессиональными ассо-

циациями.

Руководство по реализации

Членство в специальных группах или форумах должно рассматриваться как средство для:

a) повышения уровня знаний о лучших методах организации работ и текущей информационной безопасности;
b) обеспечения того, чтобы понимание среды информационной безопасности отвечало времени и было полным;
c) приёма данных оповещений о тревожных сигналах и patches, относящихся к атакам и уязвимостям;
d) получения доступа к консультациям специалиста по информационной безопасности;
e) совместное использование и обмен информацией о новых технологиях, продукции, угрозах или уязвимостях;
f) обеспечения подходящих точек взаимодействия при работе с инцидентами информационной безопасности (см. также 13.2.1).

Дополнительная информация

В целях улучшения взаимодействия и сотрудничества в области проблем безопасности могут заключаться соглашения о совместном использовании информации. В подобных соглашениях должны быть определены требования по защите секретной информации.

6.1.8 Независимый пересмотр информационной безопасности

Определение

Подход организации к управлению информационной безопасностью и её реализации (например, цели контроля, меры контроля политики, процессы и процедуры обеспечения информационной безопасности) должен периодически пересматриваться через запланированные промежутки времени или при появлении значительных изменений в реализации безопасности.

Руководство по реализации

Независимый пересмотр должен быть инициирован руководством организации. Подобные пересмотры должны проводиться лицами, не имеющими прямого отношения к пересматриваемой области безопасности, например, функция внутреннего аудита осуществляется независимым менеджером или организацией третьей стороны, специализирующейся на таких пересмотрах. Лица, проводящие эти пересмотры, должны обладать достаточными навыками и опытом.

Результаты независимого пересмотра должны регистрироваться и сообщаться руководству, которое инициировало пересмотр. Эти записи должны сохраняться.

Если при независимом пересмотре выявляется, что подход организации к управлению информационной безопасностью и его реализации неадекватен или не соответствует направлению в обеспечении информационной безопасности, определённому в документе политики информационной безопасности (см.5.1.1), руководство организации должно рассмотреть корректирующие действия.

Дополнительная информация

Область, которую менеджеры должны пересматривать регулярно (см.15.2.1) должна пересматриваться независимо. Методы пересмотра должны включать опросы руководства, проверки записей или просмотр документов политики безопасности. Руководства [7] по качеству и/или аудиту относящихся к среде систем управления могут оказать содействие при выполнении независимых пересмотров, включая выработку и реализацию программы пересмотра. В 15.3 определяются меры контроля, касающиеся независимого пересмотра операционных информационных систем и использования инструментов ауди-

та систем.

6.2 Обеспечение безопасности при наличии доступа к информационным системам сторонних организаций

Цель: поддерживать безопасность информации и средств обработки информации организации, к которым есть доступ третьих сторон, которые обрабатываются, передаются или управляются третьими (внешними) сторонами.

Безопасность информации и средств обработки информации организации не должна сокращаться введением продуктов или услуг третьих сторон.

Любой доступ к средствам обработки информации организации, обработке и передаче информации третьих сторон должен быть под контролем.

Там, где есть потребность бизнеса в работе с третьими сторонами, которые могут требовать доступа к информации и средствам обработки информации организации, или в получении или предоставлении продукта и услуги (сервиса), следует выполнять оценку риска, для определения последствий для безопасности и требований к мероприятиям по управлению информационной безопасностью. Мероприятия по управлению информационной безопасностью следует согласовывать и определять в соглашении с третьей стороной.

6.2.1 Идентификация рисков, связанных со сторонними организациями

Определение

Риски для информации и средств обработки информации организации, исходящие от бизнес-процессов, в которых участвуют сторонние организации, должны идентифицироваться, и перед предоставлением доступа к информации и средствам её обработки должны быть реализованы соответствующие средства контроля.

Руководство по реализации

Там, где есть необходимость разрешения доступа сторонней организации к информации или средствам обработки информации вашей организации, должна быть проведена оценка риска (см. также раздел 4) для определения требования по средствам контроля. При идентификации рисков, связанных с доступом третьей стороны, необходимо учитывать следующие пункты:

a) средства обработки, требуемые сторонней организацией для доступа;
b) тип доступа, который сторонняя организация будет иметь к информации и средствам обработки информации, например:
   1) физический доступ, например, к офисам, вычислительным залам, картотекам;
   2) логический доступ, например, к базам данных, информационным системам организации;
   3) сетевые соединения между сетями вашей и сторонней организацией; например, постоянное соединение, дистанционный доступ;
   4) имеет ли место доступ на территории вашей организации или вне её;
c) ценность и секретность задействованной информации и её критичность для деловых операций;
d) средства защиты, необходимые для защиты информации, не предназначенной для доступа третьей стороной;
e) персонал сторонней организации, участвующий в обработке информации вашей организации;
f) как идентифицировать организацию или персонал, санкционированные на получение доступа, как подтвердить санкционирование и как часто нужно это повторное подтверждение;

g) различные средства контроля, используемые сторонней организацией при хранении, обработке, передаче, совместном использовании и обмене информацией;
h) воздействие непредоставления доступа сторонней организации по требованию и получения его неточной или приводящей в заблуждение информации;
i) практики и процедуры, относящиеся к инцидентам нарушения информационной безопасности и нанесения потенциального ущерба, и условия для продолжения доступа сторонней организации в случае инцидента нарушения информационной безопасности;
j) законные и правовые требования и другие договорные обязательства, релевантные для сторонней организации, которые необходимо принимать во внимание;
k) как договорённости могут повлиять на интересы акционеров.

Доступ сторонних организаций к информации вашей организации не должен предоставляться, если не были реализованы соответствующие средства контроля и не подписан контракт, определяющий условия подсоединения или доступа, и рабочая договорённость. Вообще, все требования безопасности, вытекающие из работы со сторонними организациями, или внутренние средства контроля должны быть отражены в соглашении со сторонней организацией (см. также 6.2.2 и 6.2.3).

Необходимо обеспечить осведомлённость сторонней организации о её обязательствах и её принятие обязательств и обязанностей, задействованных в оценке, обработке, передаче или управлении информацией и средствами обработки информации организации.

Дополнительная информация

Информация может подвергнуться риску сторонними организациями с неадекватным управлением безопасностью. Для управления доступом сторонней организацией к средствам обработки информации необходимо определить и внедрить средства контроля. Например, если имеется особая необходимость в конфиденциальности информации, могут использоваться соглашения по неразглашению.

Организации могут подвергаться рискам, связанным с процессами внутри организации, управлением и связью, если применяется высокая степень аутсорсинга или в случае вовлечения нескольких сторонних организаций.

В 6.2.2 и 6.2.3 описываются различные договорённости со сторонними организациями, включая:

a) поставщики услуг, таких как поставщики услуг Internet, поставщики сетей, телефонные услуги, обслуживание и вспомогательные услуги;
b) услуги в обеспечении управляемой безопасностью;
c) заказчиков;
d) аутсорсинг средств и/или операций, например, систем ИТ, услуги по сбору данных, операций центра обработки вызовов;
e) консультантов и аудиторов управления и деловой деятельности;
f) разработчиков и поставщиков, например, продукции программного обеспечения и систем ИТ;
g) уборка, поставки питания и другие вспомогательные услуги, осуществляемые посторонними фирмами;
h) временный персонал, трудоустройство студентов и другие краткосрочные контракты.

Подобные договорённости могут помочь в снижении рисков, связанных со сторонними организациями.

6.2.2 Определение безопасности при работе с заказчиками

Управление

Все идентифицированные требования безопасности должны определяться перед предоставлением заказчикам доступа к информации организации или её активам.

Руководство по реализации

Следующие положения должны рассматриваться для определения безопасности до предоставления заказчикам доступа к любым активам организации (в зависимости от вида и степени доступа не все из них могут применяться):

a) защита активов, включая:
   1) процедуры по защите активов организации, в том числе информацию и программное обеспечение, и управление известными уязвимостями;
   2) процедуры для определения компрометации активов, например, вследствие потери или модификация данных;
   3) целостность;
   4) ограничения на копирование и раскрытие информации;
b) описание предоставляемого продукта ил услуги;
c) различные причины, требования и преимущества доступа заказчиков;
d) политика по управлению доступом, охватывающая:
   1) разрешенные методы доступа, а также управление и использование уникальных идентификаторов, типа пользовательских ID и паролей;
   2) процесс авторизации в отношении доступа и привилегий пользователей;
   3) утверждение, что весь доступ, который явно не санкционируется, запрещается;
   4) процесс отмены прав доступа или прерывания связи между системами;
e) процедуры отчетности, уведомления и расследования информационных неточностей (например, личные данные), инцидентов нарушения информационной безопасности и слабых звеньев системы безопасности;
f) описание каждой предоставляемой услуги;
g) определение необходимого и неприемлемого уровня обслуживания;
h) право мониторинга и блокировки любого действия, связанного с активами организации;
i) соответствующие обязательства организации и заказчика;
j) обязательства относительно юридических вопросов и того, каким образом гарантируется, что удовлетворяются юридические требования, например, законодательства о защите данных, особенно с учетом различных национальных законодательств, если соглашение относится к сотрудничеству с организациями в других странах (см также 15.1);
k) права интеллектуальной собственности (IPRs) и авторские права (см.15.1.2), а также правовая защита любой совместной работы (см. 6.1.5);

Дополнительная информация

Требования безопасности относительно заказчиков, имеющих доступ к активам организации, могут значительно варьироваться в зависимости от средств обработки информации и доступной информации. Эти требования безопасности могут адресоваться, используя договоры заказчиков, которые содержат все идентифицированные риски и требования безопасности (см.6.2.1)

Соглашения с третьими сторонами могут также включать другие стороны. Соглашения, учитывая доступ третьей стороны, должны включать разрешение для назначения других подходящих сторон и условий для их доступа и вовлечения.

6.2.3 Обеспечение безопасности в соглашениях с третьей стороной

Управление

Соглашения с третьими сторонами, включая оценку, обработку, передачу или управление информацией организации или средства обработки информации, а также добавление продукции или услуг к средствам обработки информации, должны отвечать всем требованиям безопасности.

Руководство по реализации

Соглашение должно гарантировать отсутствие недопонимания между организацией и третьей стороной. Организация должна рассматривать себя как гарантию от убытков для третьей стороны.

Для удовлетворения определённых требований безопасности (см. 6.2.1), для включения в соглашение должны быть рассмотрены следующие пункты:

a) политика информационной безопасности;
b) меры контроля для обеспечения защиты активов, включая:
   1) процедуры защиты активов организации, а именно, информацию, программное обеспечение и аппаратную часть;
   2) любые необходимые меры контроля и механизмы физической защиты;
   3) меры контроля для защиты от враждебного ПО (см. 10.4.1);
   4) процедуры определения, возникала ли какая-либо опасность для активов, например, потеря или модификация информации, ПО или аппаратной части;
   5) меры контроля для обеспечения возврата или уничтожения информации или активов в конце действия соглашения или в какой-то согласованной точке;
   6) конфиденциальность, целостность, доступность и другие соответственные свойства (см. 2.1.5) активов;
   7) ограничения по копированию и разглашению информации и использованию соглашений о конфиденциальности (см. 6.1.5);
c) обучение пользователей и администраторов методам и процедурам обеспечения безопасности;
d) обеспечение осведомлённости потребителя об информационной безопасности и проблемах её обеспечения;
e) обеспечение перехода персонала, если это необходимо;
f) обязанности, относящиеся установки и обслуживания программного обеспечения и аппаратной части;
g) чёткая структура отчётности и согласованные форматы отчёта;
h) чёткий и определённый процесс организации внесения изменений;
i) политика управления доступом, охватывающая:
   1) различные причины, требования и выгоды, которые делают доступ для третьей стороны необходимым;
   2) разрешённые методы доступа, а также контроль и применение уникальных идентификаторов, таких как идентификаторы пользователей и пароли;
   3) процесс санкционирования доступа и привилегий пользователя;
   4) требование сохранения списка лиц, санкционированных для использования сервисов, сделанных доступными, и их прав и привилегий, связанных с этим использованием;
   5) заявление, что весь доступ, который не был особо санкционирован, запрещён;
   6) процесс аннулирования прав доступа или прерывания связи между системами;
j) средства предупреждения и оповещения об инцидентах безопасности информации и нарушениях безопасности и их расследовании, а также нарушениях требований, указанных в соглашении;
k) описание поставляемых продукта или услуги и описание имеющейся в наличии

информации наряду с классификацией её безопасности (см.7.2.1);

l) намеченный уровень обслуживания и неприемлемые уровни обслуживания;

m) определение проверяемых критериев эксплуатации, их мониторинг и отчётность;

n) право контролировать и аннулировать любые действия, связанные с активами организации;

o) право ревизовать обязательства, определённые в соглашении, по проведению этих ревизий третьей стороной, и перечислять законные права аудиторов;

p) установление процесса эскалации для решения проблем;

q) требования непрерывности сервиса, включая меры обеспечения доступности и надёжности в соответствии с приоритетами организации;

r) относительные обязательства сторон перед соглашением;

s) обязательства по отношению к правовым вопросам и то, как обеспечивается соответствие правовым требованиям, например, законодательство по защите данных, особенно с учётом различных национальных правовых систем, если соглашение включает сотрудничество с организациями других стран (см. также 15.1);

t) права на интеллектуальную собственность, присвоение авторских прав (см.15.1.2) и защита любой совместной работы (см. также 6.1.5);

u) вовлечение третьей стороны с субподрядчиками и меры защиты информации, которые эти подрядчики должны реализовать;

v) условия для пересмотра условий/ аннулирования соглашений;

1) должен быть в наличии план на случай непредвиденных обстоятельств, когда любая из сторон пожелает аннулировать отношения до истечения срока действия соглашения;

2) пересмотр условий соглашений, если требования безопасности организации изменяются;

3) текущее документирование списков активов, лицензий, соглашений или связанных с ними прав.

Дополнительная информация

Соглашения для различных организаций и среди различных типов третьих сторон могут значительно отличаться. Следовательно, необходимо соблюдать осторожность при включении всех идентифицированных рисков и требований безопасности (см. также 6.2.1) в соглашения. Где это необходимо, в плане управления безопасностью требуемые меры контроля и процедуры могут быть расширены.

Если управление информационной безопасностью позаимствовано из внешних источников, в соглашениях должно быть оговорено, как третья сторона будет гарантировать поддержку адекватной безопасности, определённой оценкой рисков и как безопасность будет адаптирована для определения изменений рисков и обращения с ними.

Некоторые различия между заключением субдоговора на выполнение работ с внешними фирмами и другими формами предоставления услуг третьей стороной включают вопросы обязательств, планирования переходного периода и потенциальное разрушение хода операций во время этого периода, меры по планированию случаев непредвиденных обстоятельств и просмотров должной заботливости, а также сбор и управление информацией об инцидентах безопасности. Следовательно, важно, чтобы организация планировала и управляла переходом к соглашению с внешними фирмами, и обладала процессами управления изменениями и пересмотра условий/аннулирования соглашений.

В соглашении необходимо предусмотреть процедуры обеспечения непрерывности технологического процесса в случае, если третья сторона будет неспособна, поставлять свои услуги, чтобы избежать любой задержки при организации замещения услуг.

В соглашениях могут также участвовать другие стороны. Соглашения, предоставляющие доступ третьим сторонам, должны включать разрешение на участие других приемлемых сторон и условия их допуска и участия.

Вообще, соглашения разрабатываются в первую очередь организацией. При некоторых обстоятельствах могут быть случаи, когда соглашение может разрабатываться и возлагаться на организацию третьей стороной. Организации надо обеспечить, чтобы на её собственную безопасность не повлияли требования третьей стороны, оговоренные в налагаемых на организацию соглашениях.

7 Управление активами

7.1 Ответственность за активы

Цель: Осуществление и поддержание соответствующей защиты активов организации

Все активы подлежат учёту и должны иметь назначенного хозяина. Хозяева должны быть определены для всех активов, и должны быть распределены обязанности по поддержанию соответствующих мер защиты активов. Реализация специфических мер защиты может поручаться хозяином по обстановке, но хозяин остаётся ответственным за надлежащую защиту активов.

7.1.1 Инвентаризация активов

Определение

Все активы должны быть чётко идентифицированы, а также должна быть приведена в порядок и поддерживаться инвентаризация всех важных активов.

Руководство по реализации

Организация должна идентифицировать все активы и документировать важность этих активов. Инвентаризация активов должна включать всю информацию, необходимую для восстановления активов после какого-либо бедствия, включая тип актива, формат, местоположение, дублирующую информацию, информацию о лицензиях и ценность бизнеса. Инвентаризация не должна без необходимости дублировать другие инвентаризации, а должна обеспечивать корректировку своего содержания.

Кроме того, для каждого актива должны быть согласованы и задокументированы право собственности (см. 7.1.2) и классификация информации (см. 7.2). На основе важности актива должны определяться ценность бизнеса и категория защиты, а также уровни защиты, соответствующие важности активов (дополнительную информацию о том, как оценивать активы, чтобы представить их значимость, можно найти в [6]).

Дополнительная информация

Имеются много типов активов, включая:

a) информацию: базы данных и файлы данных, контракты и соглашения, системная документация, информация об исследованиях, руководства пользователя, учебные материалы, процедуры эксплуатации или поддержки, планы по обеспечению непрерывности деловой деятельности, процедуры отката при сбоях, контрольные журналы и архивированная информация;
b) активы программного обеспечения: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства разработки и утилиты;
c) физические активы: компьютерное оборудование, аппаратура связи, съёмные носители информации и другое оборудование;
d) услуги: вычислительные услуги и услуги связи, основные коммунальные услуги, например, отопление, освещение, подача электроэнергии, кондиционирова-

ние;

e) служащие и их квалификация, производственные опыт и навыки;

f) нематериальные факторы, такие как: репутация и престиж организации.

Описи активов дают уверенность в том, что обеспечивается эффективная защита активов, и могут также потребоваться для целей обеспечения безопасности труда, страхования или решения финансовых вопросов (управление активами). Процесс составления описи активов - важный аспект управления риском (см. также раздел 4).

7.1.2 Собственность на активы

Определение

Вся информация и активы, связанные со средствами обработки информации, должны быть в собственности* назначенного подразделения организации.

Руководство по реализации

Собственник активов должен отвечать за:

a) обеспечение соответствующей классификации информации и активов, связанных со средствами обработки информации;

b) определение и периодический пересмотр ограничений и классификаций доступа с учётом соответствующих политик контроля доступа.

Собственность может распространяться на:

a) процесс деловой деятельности;

b) определённую совокупность видов деятельности;

c) прикладную систему;

d) определённый набор данных.

Текущие задачи могут быть переданы отдельному лицу, например, куратору, надзирающему за активом на ежедневной основе, но ответственность остаётся лежать на собственнике.

В сложных информационных системах может быть полезным обозначать группы активов, которые действуют совместно для обеспечения такой определённой функции, как «услуги». В этом случае собственник услуг отвечает за поставку услуги, включая функционирование активов, которые её обеспечили.

7.1.3 Приемлемое использование активов

Определение

Правила по приемлемому использованию информации и активов, связанных со средствами обработки информации, должны быть идентифицированы, документированы и реализованы.

Руководство по реализации

Все работники, подрядчики и потребители от третьей стороны должны следовать правилам приемлемого использования информации и активов, связанных со средствами обработки информации, включая:

a) правила применения электронной почты и Интернета (см.10.8)

b) руководства по использованию переносных устройств, особенно вне пределов организации (см.11.7.1);

Специфические правила или нормы должны обеспечиваться соответствующим руководством организации. Работники, подрядчики и потребители от третьей стороны, ис-

* Термин «собственник» обозначает отдельное лицо или подразделение, которые несут административную ответственность за управление производством, разработкой, содержанием, использованием и обеспечением безопасности активов. Термин «собственник» не означает, что лицо фактически имеет какие-либо права на собственность.

пользующие или имеющие доступ к активам организации, должны быть осведомлены об ограничениях, имеющихся для их использования информации организации или активов, связанных с обработкой информации и ресурсов. Они должны нести ответственность за использование ресурсов обработки информации и любое подобное использование, выполненное под свою ответственность.

7.2 Классификация информации

Цель: Обеспечение получения информации должного уровня защиты

Информация должна быть классифицирована для указания потребности, приоритетов и ожидаемого уровня защиты при обработке информации. Информация имеет различные степени секретности и критичности. По некоторым вопросам может потребоваться дополнительный уровень защиты или специальная обработка. Для определения соответствующего набора уровней защиты и сообщения о необходимости специальных мер обращения с информацией должна применяться схема классификации информации.

7.2.1 Основные принципы классификации

Определение

Информация должна классифицироваться с точки зрения её ценности, правовых требований, секретности т критичности для организации.

Руководство по реализации

В классификации информации и связанных с ней мероприятиях по управлению информационной безопасностью следует учитывать требования бизнеса в совместном использовании или ограничении доступа к информации, и последствия для бизнеса, связанные с такими требованиями.

Основные принципы классификации должны включать условия для начальной классификации и повторной классификации по истечении некоторого времени в соответствии с некоей предопределённой политикой контроля доступа (см. 11.1.1).

Обязанностью собственника активов (см. 7.1.2) должно быть определение классификации актива, периодический её пересмотр и поддержание её на современном уровне. При классификации должен учитываться эффект агрегирования, упомянутый в 10.7.2.

Необходимо высказать некоторые соображения относительно числа классификационных категорий и преимуществ, получаемых от их использования. Чрезмерно сложные схемы могут стать обременительными и неэкономичными для использования, или оказываются неосуществимыми. Следует проявлять осмотрительность при интерпретации категорий (грифов) классификации на документах от других организаций, которые могут иметь другие определения для тех же самых или подобных категорий.

Дополнительная информация

Уровень защиты можно оценить посредством анализа конфиденциальности, целостности, доступности и любых других требований для рассматриваемой информации.

Информация часто перестает быть чувствительной или критичной по истечении некоторого периода времени, например, когда информация сделана общедоступной. Эти аспекты следует принимать во внимание, поскольку присвоение повышенной категории может привести к задействованию излишних мер защиты, таким образом, увеличивая расходы.

При присвоении уровней секретности совместное рассмотрение документов с одинаковыми требованиями безопасности может помочь упростить задачу по засекречиванию.

Вообще, засекреченность информации является стенографическим способом определения, как эта информация должна быть обработана и защищена.

7.2.2 Маркировка и обработка информации

Определение

Для маркировки и обработки информации должен быть разработан набор процедур в соответствии со схемой засекречивания, принятой организацией.

Руководство по реализации

Процедуры маркировки информации должны охватывать информационные активы в физических и электронных форматах.

При осуществлении вывода данных из систем, содержащих информацию, которая классифицирована как чувствительная или критичная, следует использовать соответствующую пометку классификации (при выводе). В маркировке следует отражать классификацию согласно 7.2.1. Следует рассматривать напечатанные отчеты, экранные формы, носители информации (ленты, диски, компакт-диски, кассеты), электронные сообщения и передачу файлов.

Для каждого уровня секретности должны быть определены процедуры обработки, включающие безопасную обработку, хранение, передачу, рассекречивание и уничтожение. Сюда следует также отнести процедуры по обеспечению сохранности и регистрации любого события, имеющего значение для безопасности.

Соглашения с другими организациями, включающие совместное использование информации, должны включать процедуры определения засекреченности этой информации и интерпретации грифов секретности других организаций.

Дополнительная информация

Маркировка и безопасная обработка засекреченной информации является главным требованием для договорённостей по совместному использованию информации. Физические пометки являются основной формой маркировки. Однако, некоторые информационные активы, такие как: документы в электронном виде, физически невозможно маркировать и необходимо применять электронные средства маркировки. Например, на экране или дисплее отметка об уведомлении может появиться. Там, где маркировка невозможна, могут применяться другие средства обозначения засекреченности информации, например, посредством процедур или метаданных.

8 Вопросы безопасности, связанные с кадровыми ресурсами

8.1 Перед трудоустройством*

Цель: Обеспечение понимания работниками, подрядчиками и потребителями третьей стороны своих обязательств и соответствия ролям, для которых они предназначены, в целях снижения риска как следствия кражи, мошенничества или неправильного использования средств обработки информации.

Обязательства по обеспечению безопасности должны быть представлены до найма в адекватных должностных инструкциях, а также в условиях договора по найму.

Все кандидаты для найма, подрядчики и пользователи третьей стороны должны быть тщательно проверены, особенно для секретных работ.

Работники, подрядчики и пользователи третьей стороны средств обработки информации должны подписывать договор о своих ролях и обязанностях.

* Под словом «трудоустройство» понимаются следующие ситуации: работа по найму (временная или постоянная), назначение на должность, изменение должности, переуступки контрактов и аннулирование любого из этих условий.

8.1.1 Роли и обязательства

Определение

Роли и обязательства работников, подрядчиков и пользователей третьей стороны по обеспечению безопасности должны определяться и документироваться в соответствии с политикой информационной безопасности.

Руководство по реализации

Роли и обязанности по обеспечению безопасности должны включать требование по:

a) реализации и действиям в соответствии с политиками информационной безопасности организации (см. 5.1);
b) защите активов от несанкционированного доступа, разглашения, изменения, уничтожения или вмешательства;
c) выполнению особых процессов или действий по обеспечению безопасности;
d) обеспечению назначения обязанностей на определённые лица;
e) сообщению о событиях безопасности, потенциальных событиях и других рисках безопасности для организации.

Роли и обязанности по обеспечению безопасности должны быть чётко определены и доведены до кандидатов на получение работы перед процессом найма.

Дополнительная информация

Для документирования ролей и обязанностей по обеспечению безопасности должны использоваться должностные инструкции. Роли и обязанности по обеспечению безопасности для лиц, не нанятых через процесс по трудоустройству организации, т.е. нанятых через организацию третьей стороны, также должны быть чётко определены и доведены.

8.1.2 Проверка

Определение

Проверки происхождения всех кандидатов на трудоустройство, подрядчиков и пользователей третьей стороны должны проводиться в соответствии с правовыми и этическими нормами и соразмерно требованиям бизнеса, засекреченности информации, к которой они будут допущены, и воспринимаемым рискам.

Руководство по реализации

При проверках должны приниматься во внимание личная жизнь, защита персональных данных и законодательство по трудоустройству и, где разрешено, эти проверки должны включать:

a) наличие положительных рекомендаций, в частности в отношении деловых и личных качеств претендента;
b) проверку (на предмет полноты и точности) резюме претендента;
c) подтверждение заявляемого образования и профессиональных квалификаций;
d) независимую проверку подлинности документов, удостоверяющих личность паспорта или заменяющего его документа);
e) более подробные проверки, такие как проверки счетов в банке или проверки на криминальное прошлое.

В случаях, когда новому сотруднику непосредственно после приема на работу или в дальнейшем предстоит доступ к средствам обработки информации, и, в особенности, если эта информация является важной, например, финансовая информация или совершенно секретная информация, организации следует предусмотреть возможность проведения более подробных проверок.

В процедурах проверок должны быть определены критерии и ограничения, например, кто имеет право на проверку и как, где и почему проводить проверки.

Процесс проверки следует осуществлять для подрядчиков и пользователей третьей стороны. В тех случаях, когда найм сотрудников осуществляется через кадровое агентст-

во, контракт с агентством должен четко определять обязанности агентства по проверке претендентов и процедурам уведомления, которым оно должно следовать, если проверка не была закончена или, если результаты дают основания для сомнения или беспокойства. Подобным образом, в соглашении с третьей стороной (см. также 6.2.3) должны точно быть обозначены все обязанности и процедуры уведомления для проверки.

Информация по всем претендентам на должности внутри организации должна собираться и обрабатываться в соответствии с надлежащим законодательством, существующим в релевантной юрисдикции. В зависимости от применяемого законодательства претенденты должны быть заранее проинформированы о проверках.

8.1.3 Условия трудового соглашения

Определение

Как часть договорного обязательства работники, подрядчики и пользователи третьей стороны должны согласовать и подписать условия своего трудового соглашения, которые должны определять их обязанности и обязанности организации в отношении информационной безопасности.

Руководство по реализации

Условия трудового соглашения должны отражать политику безопасности организации, кроме разъяснения и формулирования, что:

a) все работники, подрядчики и пользователи третьей стороны, которым предоставляется доступ к засекреченной информации, перед предоставлением им доступа к средствам обработки информации должны подписать соглашение о конфиденциальности и неразглашении;
b) юридические права и обязанности работника, подрядчика и пользователя третьей стороны, например, относительно авторских прав или закон о защите данных (см. также 15.1.1 и 15.1.2);
c) ответственность за засекреченность информации и управление активами организации, связанными с информационными системами и услугами, с которыми работают служащие, подрядчик или пользователь третьей стороны (см. также 7.2.1 и 10.7.3);
d) ответственности работника, подрядчика или пользователя третьей стороны за обработку информации, полученной от других компаний или внешними сторонами;
e) ответственность организации за обработку персональной информации, включая персональную информацию, полученную в результате или в ходе работы на организацию (см. также 15.1.4);
f) ответственность при работе за пределами помещения организации и сверхурочного времени, например, в случае работы на дому (см. также 9.2.5 или 11.7.1);
g) действия, которые предпринимаются в случае, если работник, подрядчик или пользователь третьей стороны игнорируют требования безопасности организации (см. 8.2.3).

Организация должна обеспечить согласие работников, подрядчиков и пользователей третьей стороны с условиями, касающимися информационной безопасности, по отношению к сущности и степени доступа, который они будут иметь к активам организации, связанных с информационными службами и системами.

Где это целесообразно, обязательства, указанные в условиях трудового соглашения, должны иметь силу в течение определенного периода времени после окончания действия трудового соглашения (см. также 8.3).

Дополнительная информация

Для охвата обязательств работника, подрядчика или пользователя третьей стороны, относящихся к конфиденциальности, защите данных, этике, должному использованию оборудования и техники организации, а также правилам, приемлемым для организации, может использоваться кодекс поведения. Подрядчик и пользователи третьей стороны могут быть связаны с какой-либо внешней организацией, которая в свою очередь может потребоваться для входа в договорные соглашения от имени законтрактованного лица.

8.2 Во время работы по трудовому соглашению

Цель: Обеспечение осведомлённости работников, подрядчиков и пользователей третьей стороны об угрозах и проблемах для информационной безопасности и их обеспеченности всем необходимым для поддержки политики информационной безопасности организации при выполнении служебных обязанностей и снижение риска вследствие человеческого фактора.

Для обеспечения соблюдения безопасности в течение всего периода работы лица в организации определяются административные ответственности.

Для сведения к минимуму возможных рисков безопасности всем работникам, подрядчикам и пользователям третьей стороны должен быть обеспечен адекватный уровень осведомлённости, обучения и профессиональной подготовки по отношению к процедурам обеспечения безопасности и правильного использования средств обработки информации. Для рассмотрения нарушений безопасности должен быть выработан дисциплинарный процесс.

8.2.1 Административная ответственность

Определение

Руководство организации должно требовать от работников, подрядчиков и пользователей третьей стороны поддержания безопасности в соответствии с установленными политиками и процедурами организации.

Руководство по реализации

Административная ответственность должна включать гарантию того, чтобы работники, подрядчики и пользователи третьей стороны были:

a) должным образом проинструктированы о ролях и обязательствах по отношению к информационной безопасности до предоставления им доступа к секретной информации или информационным системам;
b) обеспечены руководствами по определению их роли по отношению к безопасности внутри организации;
c) мотивированы для выполнения политик безопасности организации;
d) способны достичь уровня осведомлённости, относящейся к их ролям и обязанностям внутри организации (см. также 8.2.2);
e) способны соответствовать условиям трудового соглашения, которое включает политику информационной безопасности организации и собственные режимы работы;
f) способны продолжать совершенствовать навыки и квалификацию.

Дополнительная информация

Если работники, подрядчики и пользователи третьей стороны не осведомлены о своих обязательствах по отношению к безопасности, они могут нанести значительный ущерб организации. Очевидно, мотивированный персонал будет более надёжен и создаёт меньше инцидентов нарушения информационной безопасности.

Неудовлетворительное управление организацией может вызвать у персонала чувство недооценки, что отрицательно сказывается на безопасности организации. Например, не-

удовлетворительное управление может привести к игнорированию безопасности или потенциальному неправильному использованию активов организации.

8.2.2 Осведомлённость, обучение и подготовка в области информационной безопасности

Определение

Все сотрудники организации и, при необходимости, пользователи третьей стороны, должны пройти соответствующее обучение и получать на регулярной основе обновленные варианты политик и процедур информационной безопасности, принятых в организации, в соответствии с их должностными функциями.

Руководство по реализации

Подготовка в области осведомлённости должна начинаться с процесса введения предназначенного для ознакомления с политиками информационной безопасности и ожиданиями организации перед предоставлением доступа к информации или службам.

Последующая подготовка должна включать изучение требований безопасности, юридических обязательств и мер контроля деловой деятельности, а также обучение правильному использованию средств обработки информации, например, процедуре регистрации в системах, применению пакетов программ, и информацию о дисциплинарном процессе (см. 8.2.3)

Дополнительная информация

Действия по обучению, подготовке и обеспечению осведомлённости об информационной безопасности должны соответствовать роли лица, его обязанностям и рабочим навыкам и включать информирование по известным угрозам, с кем контактировать для проведения консультаций по безопасности и каналам сообщения об инцидентах нарушения информационной безопасности (см. также 13.1)

Подготовка по улучшению осведомлённости имеет целью дать возможность отдельным лицам распознавать проблемы информационной безопасности и инциденты её нарушения и реагировать соответственно своим рабочим обязанностям.

8.2.3 Дисциплинарный процесс

Определение

Для сотрудников, нарушивших безопасность, должен существовать надлежаще оформленный дисциплинарный процесс.

Руководство по реализации

Дисциплинарный процесс нельзя начинать без подтверждения нарушения безопасности (информацию по сбору свидетельств см. 13.2.3).

Официальный дисциплинарный процесс должен гарантировать корректное и справедливое отношение к работникам, подозреваемым в нарушении безопасности. Официальный дисциплинарный процесс должен обеспечивать дифференцированную реакцию, учитывая такие факторы, как характер и серьёзность нарушения и его воздействия на деловую деятельность независимо от того, первое это или повторное нарушение, уровень подготовки нарушителя, релевантное законодательство, деловые контракты и другие факторы. В случаях серьёзных нарушений должностных обязанностей процесс должен предусматривать немедленное аннулирование служебных обязанностей, прав доступа и привилегий доступа и при необходимости немедленный вывод нарушителя из расположения организации.

Дополнительная информация

Дисциплинарный процесс должен также применяться как сдерживающее средство для предотвращения нарушения работниками, подрядчиками и пользователями третьей стороны политик и процедур безопасности организации и любых других нарушений безо-

пасности.

8.3 Прекращение действия трудового соглашения или его изменение

Цель: обеспечение выхода работников, подрядчиков и пользователей третьей стороны из организации или изменение их трудового соглашения в организованном порядке.

Должны быть распределены обязанности по управлению выходом работников, подрядчиков или пользователей третьей стороны из организации, возвратом всего оборудования и аннулированием всех прав доступа.

Изменение обязанностей и трудовых соглашений внутри организации должны рассматриваться как окончание действия соответствующих обязанностей или трудового соглашения в соответствии с этим разделом и любые новые трудовые соглашения должны руководствоваться описанием 8.1

8.3.1 Обязанности по окончании действия трудового соглашения

Определение

Обязанности по выполнению прекращения трудового соглашения или изменению трудового соглашения должны быть чётко определены и распределены.

Руководство по реализации

Передача обязанностей при окончании действия трудовых соглашений должно включать действующие требования безопасности, правовые обязательства, где это приемлемо, обязанности, содержащиеся в любом соглашении о конфиденциальности (см. 6.1.5) и условиях трудового соглашения, действующих в течение определенного времени по истечении трудового соглашения работника, подрядчика или пользователя третьей стороны.

Обязательства и обязанности, всё ещё имеющие силу после окончания трудового соглашения, должны быть включены в контракты работника, подрядчика или пользователя третьей стороны.

Изменения в обязанностях или трудовых соглашениях должны рассматриваться как окончание соответствующей обязанности или трудового соглашения, а новая обязанность или трудовое соглашение должны контролироваться, как описано в 8.1.

Дополнительная информация

В основном за процесс окончания трудового соглашения несёт ответственность отдел кадров, который работает вместе с руководителем лица, назначенного управлять аспектами безопасности релевантных процедур. В случае с подрядчиком ответственность за процедуру завершения трудового соглашения может нести организация, ответственная за подрядчика, а в случае с другим пользователем ответственность несёт его организация.

Может возникнуть необходимость в информировании работников, заказчиков, подрядчиков или пользователей третьей стороны об изменениях среди персонала и в оперативных мероприятиях.

8.3.2 Возврат активов

Определение

Все работники, подрядчики и пользователи третьей стороны должны возвратить все активы организации, находящиеся в их владении, после окончания их трудового соглашения, контракта или договора.

Руководство по реализации

Процесс оформления окончания трудового соглашения должен быть формализован для возврата всего ранее выданного программного обеспечения, корпоративных документов и оборудования. Необходимо также возвратить все активы организации, такие как переносные вычислительные устройства, кредитные карточки, карточки доступа, программ-

ное обеспечение руководства и информацию, хранящуюся на электронных носителях.

В случаях, когда работник, подрядчик или пользователь покупает оборудование организации или использует своё личное оборудование, необходимо использовать процедуры обеспечения передачи организации всей релевантной информации и её надёжного стирания с оборудования (см. также 10.7.1).

В случаях, когда работник, подрядчик или пользователь третьей стороны обладает информацией, имеющей значение для текущих операций, эта информация должна документироваться и передаваться организации.

8.3.3 Аннулирование прав доступа

Определение

Права доступа всех работников, подрядчиков и пользователей третьей стороны к информации и средствам обработки информации должны быть аннулированы после окончания их трудового соглашения, контракта или договора или их исправления после внесения изменений.

Руководство по реализации

По окончании трудового соглашения права доступа отдельного лица к активам, связанным с информационными системами и службами, должны быть предусмотрены. При этом определяется необходимость аннулирования прав доступа. Изменения в трудовом соглашении должны быть отражены в аннулировании всех прав доступа, которые не были утверждены для нового трудового соглашения. Права доступа, которые должны аннулироваться или адаптироваться, включают физический и логический доступ, ключи, идентификационные карты, средства обработки информации (см. также 11.2.4), подписки и устранение из любой документации, которая идентифицирует их (работника, подрядчика, пользователя третьей стороны) как действующего члена организации. Если увольняющийся работник, подрядчик или пользователь третьей стороны знает пароль к активным счетам, эти пароли должны быть изменены после окончания или изменения трудового соглашения, контракта или договора.

Права доступа к информационным активам и средствам обработки информации должны быть сокращены или аннулированы до окончания или изменения трудового соглашения в зависимости от оценки таких факторов риска, как:

a) было ли окончание трудового соглашения или его изменение инициировано работником, подрядчиком или пользователем третьей стороны или руководством организации и причины окончания;
b) текущие обязанности работника, подрядчика и пользователя третьей стороны;
c) ценность доступных в данное время активов.

Дополнительная информация

При определённых обстоятельствах права доступа могут распределяться на основе доступности нескольким людям, кроме увольняющихся работника, подрядчика или пользователя третьей стороны, например, групповые идентификаторы. В подобных случаях увольняющиеся лица должны быть удалены из списков группового доступа и должны быть приняты меры, чтобы оставшиеся в группе работники, субподрядчики и пользователи третьей стороны больше не делились информацией с увольняющимся лицом.

В случае с окончанием трудового соглашения, инициированного руководством организации, потерявшие доверие работники, подрядчики, пользователи третьей стороны могут намеренно разрушить информацию или саботировать средства обработки информации. В случае подачи в отставку лиц последние могут поддаться соблазну собрать информацию для использования в будущем.

9 Физическая защита и защита от воздействий окружающей среды

9.1 Охраняемые зоны

Цель: предотвращение несанкционированного физического доступа, повреждения и воздействия в отношении помещений и информации организации.

Средства обработки критичной или важной служебной информации необходимо размещать в зонах безопасности, обозначенных определенным периметром безопасности, обладающим соответствующими защитными барьерами и средствами контроля проникновения. Эти зоны должны быть физически защищены от несанкционированного доступа, повреждения и воздействия.

Уровень защищенности должен быть соразмерен с идентифицированными рисками.

9.1.1 Периметр физической защиты

Определение

Для защиты зон, содержащих информацию или средства обработки информации, должны использоваться периметры безопасности (барьеры, такие как стены, контролируемые входы по карточкам или сотрудник у стойки регистрации).

Руководство по реализации

Рекомендуется рассматривать и внедрять при необходимости следующие меры (средства) контроля для физической защиты периметра:

a) периметр безопасности должен быть четко определен, и расположение и сила каждого периметра должны зависеть от требований безопасности активов в периметре и результатов оценки риска;

b) периметр здания или помещений, где расположены средства обработки информации, должен быть физически сплошным (то есть, не должно быть никаких промежутков в периметре или мест, через которые можно было бы легко проникнуть). Внешние стены помещений должны иметь достаточно прочную конструкцию, а все внешние двери должны быть соответствующим образом защищены от неавторизованного доступа, например, оснащены устройствами контроля доступа, шлагбаумами, сигнализацией, замками и т.п.; двери и окна должны закрываться пока не задействуются, и внешняя защита окон должна рассматриваться, особенно на уровне земли;

c) должна быть выделенная и укомплектованная персоналом зона регистрации посетителей или существовать другие мероприятия по управлению информационной безопасностью физического доступа в помещения или здания. Доступ в помещения и здания должен быть предоставлен только авторизованному персоналу;

d) где это приемлемо, надо воздвигнуть физические барьеры для предотвращения несанкционированного физического доступа и загрязнения окружающей среды;

e) все противопожарные выходы в периметре безопасности должны быть оборудованы аварийной сигнализацией, проверены и испытаны вместе со стенами для установления необходимого уровня сопротивления в соответствии с региональными, национальными и международными стандартами; они должны безотказно функционировать в соответствии с местными противопожарными правилами;

f) соответствующие системы обнаружения нарушителя должны быть установлены по национальным, региональным или международным стандартам на всех наружных дверях и доступных окнах и должны регулярно испытываться; неза-

нятые помещения всё время должны быть под охраной сигнализации; для других зон, например, машинный зал или помещение связи;

g) средства обработки информации организации должны быть физически отделены от средств обработки третьих сторон.

Дополнительная информация

Физическую защиту можно осуществить путём создания одного или нескольких физических барьеров вокруг помещений организации и средств обработки информации. Применение нескольких барьеров обеспечивает дополнительную защиту, и отказ одного из барьеров не означает создания немедленной угрозы для безопасности.

Физическая защита доступа в здания, в которых размещены несколько организаций, требует специального рассмотрения.

9.1.2 Контроль доступа в охраняемые зоны

Определение

Зоны информационной безопасности необходимо защищать с помощью соответствующих мер контроля входа, с тем, чтобы обеспечивать уверенность в том, что доступ позволен только авторизованному персоналу.

Руководство по реализации

Необходимо рассмотреть следующие правила:

a) необходимо регистрировать дату и время входа и выхода посетителей и все посетители должны быть под наблюдением, если их доступ не был заранее утверждён, доступ для них должен предоставляться только для специальных санкционированных целей, и для них должны быть созданы инструкции по требованиям безопасности зоны и чрезвычайным процедурам.

b) доступ к зонам, в которых обрабатывается или хранится секретная информация, должен контролироваться и предоставляться только авторизованным лицам; следует использовать средства аутентификации, например, карты доступа плюс PIN-код для авторизации и предоставления соответствующего доступа. Необходимо также надежным образом проводить аудит журналов регистрации доступа;

c) необходимо требовать от всех работников, подрядчиков и пользователей третьей стороны и всех посетителей ношения признаков видимой идентификации, а также немедленного оповещения работников службы безопасности в случае встречи посетителей без сопровождения и кого-либо без идентифицирующих признаков;

d) вспомогательному персоналу третьей стороны должен предоставляться ограниченный доступ к зонам безопасности или средствам обработки секретной информации только при необходимости; этот доступ должен быть санкционирован и контролироваться;

e) права доступа к зонам безопасности должны регулярно пересматриваться и обновляться и при необходимости аннулироваться (см. 8.3.3).

9.1.3 Обеспечение безопасности офисов, рабочих помещений и оборудования

Определение

Должна быть разработана и реализована физическая безопасность офисов, рабочих помещений и оборудования.

Руководство по реализации

Для защиты офисов, рабочих помещений и оборудования должны быть рассмотрены следующие правила:

a) следует принимать в расчет соответствующие правила и стандарты в отноше-

нии охраны здоровья и безопасности труда;

b) основное оборудование должно быть расположено в тех местах, где ограничен доступ посторонних лиц;

c) здания не должны выделяться на общем фоне и должны иметь минимальные признаки своего назначения; не должны иметь очевидных вывесок вне или внутри здания, по которым можно сделать вывод о выполняемых функциях обработки информации;

d) справочники и внутренние телефонные книги, идентифицирующие местоположения средств обработки важной информации, не должны быть доступны посторонним лицам.

9.1.4 Защита от внешних угроз и угроз от окружающей среды

Определение

Должна быть создана и реализована физическая защита от пожара, наводнения, землетрясения, взрыва, гражданского неповиновения и других форм природных и антропогенных катастроф.

Руководство по реализации

Необходимо рассмотреть любые угрозы безопасности, исходящие от соседних помещений, например, пожар в соседнем здании, протекание воды через крышу или через пол из подземных уровней или уличный взрыв.

Для избежания ущерба от пожара, наводнения, землетрясения, взрыва, гражданского неповиновения и других видов природных и антропогенных катастроф необходимо рассмотреть следующие правила:

a) следует обеспечить надежное хранение опасных или горючих материалов на достаточном расстоянии от зоны информационной безопасности. Большие запасы бумаги для печатающих устройств не следует хранить в зоне безопасности;

b) резервное оборудование и носители данных следует располагать на безопасном расстоянии во избежание повреждения от последствий стихийного бедствия в основном здании;

c) должен быть предусмотрен и удобно размещён противопожарный инвентарь.

9.1.5 Выполнение работ в охраняемых зонах

Определение

Должна быть создана и реализована физическая защита и правила проведения работ в охраняемых зонах.

Руководство по реализации

Необходимо рассмотреть следующие правила:

a) о существовании зоны информационной безопасности и проводимых там работах должны быть осведомлены только те лица, которым это надо в силу производственной необходимости;

b) из соображений безопасности и предотвращения возможности злонамеренных действий в охраняемых зонах необходимо избегать случаев работы без надлежащего контроля со стороны уполномоченного персонала;

c) пустующие зоны безопасности должны быть физически заперты и их состояние необходимо периодически проверять;

d) использование фото, видео, аудио или другого записывающего оборудования (такого как камеры в мобильных телефонах) должно быть запрещено, если только не получено на то специальное разрешение.

Мероприятия по выполнению работ в охраняемых зонах включают контроль за ра-

ботниками, подрядчиками и пользователями третьей стороны, работающими в охраняемых зонах, а также деятельностью третьей стороны в этих зонах.

9.1.6 Зоны доступа к местам общественного пользования, приемки и отгрузки материальных ценностей

Определение

Такие места доступа, как зоны приёмки и отгрузки, и другие места, где несанкционированные лица могут проникнуть на территорию организации, должны находиться под контролем и, по возможности, быть изолированы от средств обработки информации с целью избежания несанкционированного доступа.

Руководство по реализации

Необходимо рассмотреть следующие правила:

a) доступ к местам приёмки и отгрузки материальных ценностей с внешней стороны здания должен быть разрешен только определенному и авторизованному персоналу;
b) места приёмки и отгрузки материальных ценностей должны быть организованы так, чтобы поступающие материальные ценности могли быть разгружены без предоставления персоналу поставщика доступа к другим частям здания;
c) должна быть обеспечена безопасность по отношению к внешним дверям помещения для приёмки и отгрузки должны, когда внутренние двери открыты;
d) поступающие материальные ценности должны быть осмотрены на предмет потенциальных опасностей (см.9.2.1d)) прежде, чем они будут перемещены из помещения для приёмки и отгрузки к местам использования;
e) поступающие материальные ценности должны быть зарегистрированы, в соответствии с процедурами управления активами (см. также 7.1.1);
f) по возможности, поступающие и отправляемые грузы должны быть разделены.

9.2 Безопасность оборудования

Цель: предотвращение потерь, повреждений, хищений или созданий угрозы для активов и прерывания деятельности организации.

Оборудование необходимо защищать от угроз его безопасности и воздействий окружающей среды.

Обеспечение безопасности оборудования (включая и то, что используется вне организации и ликвидацию собственности) необходимо, чтобы уменьшить риск неавторизованного доступа к информации и защитить их от потери или повреждения. При этом необходимо принимать во внимание аспекты, связанные с расположением оборудования и случаями его перемещения. Могут потребоваться специальные мероприятия защиты от опасных воздействий среды или неавторизованного доступа через инфраструктуры обеспечения, в частности, системы электропитания и кабельной разводки.

9.2.1 Расположение и защита оборудования

Определение

Оборудование должно быть расположено или защищено так, чтобы уменьшить риски от воздействий окружающей среды, и возможности несанкционированного доступа.

Руководство по реализации

Необходимо рассматривать следующие мероприятия по защите оборудования:

a) оборудование необходимо размещать таким образом, чтобы свести до минимума излишний доступ в места его расположения;
b) средства обработки важной информации, следует размещать так, чтобы

уменьшить риск несанкционированного наблюдения за их функционированием и средства хранения должны защищаться во избежание несанкционированного доступа;

c) отдельные элементы оборудования, требующие специальной защиты, необходимо изолировать, чтобы повысить общий уровень необходимой защиты;

d) мероприятия по управлению информационной безопасностью должны быть внедрены таким образом, чтобы свести к минимуму риск потенциальных угроз, например, воровство, пожар, взрыв, задымление, затопление (или перебои в подаче воды), пыль, вибрация, химические эффекты, помехи в электроснабжении, помехи в средствах связи, электромагнитное излучение и вандализм;

e) необходимо разработать правила приёма пищи и курения вблизи средств обработки информации;

f) следует проводить мониторинг состояния окружающей среды по выявлению условий, которые могли бы неблагоприятно влиять на функционирование средств обработки информации;

g) все здания должны быть оснащены громоотводами, а все внешние линии связи оборудованы специальными грозозащитными фильтрами;

h) в отношении оборудования, расположенного в производственных цехах следует использовать специальные средства защиты, например, защитные пленки для клавиатуры;

i) оборудование, обрабатывающее секретную информацию, должно иметь защиту для сведения к минимуму риска утечки информации в результате излучения.

9.2.2 Вспомогательные коммунальные услуги

Определение

Оборудование должно быть защищено от отключения электричества и других нарушений работы, вызываемых сбоями в системе коммунальных услуг.

Руководство по реализации

Все вспомогательные коммунальные услуги, также как электричество, водоснабжение, канализация, отопление/вентиляция и кондиционирование воздуха должны быть адекватны системам, которые они обслуживают. Вспомогательные коммунальные услуги должны проходить регулярную проверку и, по возможности, испытание с целью обеспечения их должного функционирования и понижения риска их неправильного срабатывания или сбоев. Необходимо наличие источника питания, технические данные которого соответствуют спецификациям производителя оборудования. Необходимо обеспечивать надлежащую подачу электропитания, соответствующую спецификациям производителя оборудования.

Чтобы обеспечить безопасное выключение и/или непрерывное функционирование устройств, через UPS рекомендуется подключать оборудование, поддерживающее критические бизнес процессы. В планах обеспечения непрерывности следует предусматривать действия, которые должны быть предприняты при отказе UPS. Оборудование UPS следует регулярно проверять на наличие адекватной мощности, а также тестировать в соответствии с рекомендациями производителя. UPS и генераторы должны регулярно проверяться на наличие адекватной мощности и испытываться в соответствии с рекомендациями производителя. Кроме того, необходимо рассмотреть возможность использования нескольких источников питания или, если территория организации достаточно велика, отдельной электроподстанции.

Аварийные выключатели электропитания необходимо располагать около запасных выходов помещений, где расположено оборудование, чтобы ускорить отключение электропитания в случае критических ситуаций. Необходимо обеспечить работу аварийного

освещения на случай отказа электропитания, потребляемого от сети.

Водоснабжение должно быть стабильным и адекватным для питания кондиционеров воздуха, увлажнителей воздуха и систем пожаротушения (если таковые имеются). Неправильное срабатывание системы водоснабжения может повредить оборудование или нарушить эффективность работы системы пожаротушения. Если потребуется, надо установить систему сигнализации для обнаружения сбоев в системах вспомогательных коммуникационных услуг.

Телекоммуникационное оборудование должно соединяться с поставщиком, по крайней мере, двумя обходными маршрутами для предотвращения отказа на одном.

Дополнительная информация

Варианты обеспечения непрерывности работы источников питания включают несколько фидеров для избежания сбоя в подаче питания.

9.2.3 Безопасность кабельной сети

Определение

Силовые и телекоммуникационные кабельные сети, по которым передаются данные или осуществляются другие информационные услуги, необходимо защищать от перехвата информации или повреждения.

Руководство по реализации

Должны быть рассмотрены следующие правила:

a) силовые и телекоммуникационные линии, связывающие средства обработки информации, должны быть, по возможности, подземными или обладать адекватной альтернативной защитой;
b) сетевой кабель должен быть защищен от неавторизованных подключений или повреждения, например, посредством использования специального кожуха и/или выбора маршрутов прокладки кабеля в обход общедоступных участков;
c) силовые кабели должны быть отделены от коммуникационных, чтобы предотвращать помехи;
d) для сведения к минимуму возможности ошибок из-за неправильного обращения, таких как сращивание неправильных сетевых кабелей, необходимо применять легко распознаваемые маркировки на кабелях и оборудовании;
e) должен применяться перечень временных соединений для уменьшения вероятности появления ошибок;
f) для секретных или критических систем рассматриваемые меры защиты включают:
   1) использование бронированных кожухов, а также закрытых помещений/ящиков в промежуточных пунктах контроля и конечных точках;
   2) использование дублирующих маршрутов прокладки кабеля и/или альтернативных способов передачи, обеспечивающих соответствующую защиту;
   3) использование оптико-волоконных линий связи;
   4) использование электромагнитного экранирования для защиты кабелей;
   5) проверки на технические подключения и физические экспертизы неавторизованных устройств к кабельной сети;
   6) контролируемый доступ к коммутационным панелям и помещениям для кабелей.

9.2.4 Техническое обслуживание оборудование

Определение

В организации должно проводиться надлежащее техническое обслуживание оборудования для обеспечения его непрерывной работоспособности и целостности.

Руководство по реализации

Для обслуживания оборудования необходимо рассмотреть следующие правила:

a) оборудование следует обслуживать в соответствии с рекомендуемыми поставщиком периодичностью и инструкциями;
b) необходимо, чтобы техническое обслуживание и ремонт оборудования проводились только авторизованным персоналом;
c) следует хранить записи обо всех случаях предполагаемых или фактических неисправностей и всех видах профилактического и восстановительного технического обслуживания;
d) когда оборудование запланировано для обслуживания, должны задействоваться соответствующие меры защиты с учётом проведения обслуживания персоналом организации или посторонним персоналом; где необходимо, секретная информация должна быть удалена из оборудования или обслуживающий персонал должен подвергнуться тщательной проверке;
e) должны соблюдаться все требования, устанавливаемые использующимися правилами страхования.

9.2.5 Обеспечение безопасности оборудования, используемого вне помещений организации

Определение

Меры безопасности должны применяться по всему оборудованию, используемому за пределами организации с учётом различных рисков, связанных с работами вне помещений организации.

Руководство по реализации

Независимо от принадлежности оборудования, его использование для обработки информации вне помещения организации должно быть авторизовано руководством.

Для защиты оборудования, используемого вне помещений организации, должны рассматриваться следующие правила:

a) оборудование и носители информации, взятые из помещений организации, не следует оставлять без присмотра в общедоступных местах. При путешествиях компьютеры следует перевозить как ручную кладь и, по возможности, не афишировать ее содержимое;
b) всегда необходимо соблюдать инструкции изготовителей по защите оборудования, например, от воздействия сильных электромагнитных полей;
c) при работе дома следует применять подходящие мероприятия по управлению информационной безопасностью с учетом оценки рисков, например, использовать запираемые файл-кабинеты, соблюдать политику "чистого стола" и контролировать возможность доступа к компьютерам и безопасной связи с офисом (см. также [8] Сетевая безопасность);
d) должны иметь место адекватные меры по страхованию для защиты оборудования вне помещений организации.

Риски безопасности, например, связанные с повреждением, воровством и подслушиванием, могут значительно зависеть от расположения и должны учитываться при определении наиболее подходящих мероприятий по управлению информационной безопасностью.

Дополнительная информация

Оборудование по обработке и хранению информации включает все типы персональных компьютеров, электронных записных книжек, мобильных телефонов, кредитных карточек, а также бумаги или иные материальные ценности, которое используются для работы на дому или транспортируются за пределы рабочих помещений.

9.2.6 Безопасная утилизация или повторное использование оборудования

Определение

Все компоненты оборудования, содержащего носители данных, следует проверять, чтобы убедиться, что все секретные данные и лицензированные программные обеспечения удалены или безопасным образом переписаны перед уничтожением.

Руководство по реализации

Устройства, содержащие секретную информацию, должны быть физически уничтожены, а информация должна быть уничтожена, стёрта или переписана с помощью методов, делающих исходную информацию невосстанавливаемой вместо использования стандартной функции стирания или формата.

Дополнительная информация

Для повреждённых устройств, содержащих секретные данные, может потребоваться оценка риска для определения, необходимо ли физическое уничтожение элементов вместо их ремонта или отбраковки.

Информации может угрожать опасность вследствие небрежности использования или повторного применения (см. также 10.7.2)

9.2.7 Вынос имущества

Определение

Оборудование, информацию или программное обеспечение нельзя выносить из помещения без предварительного разрешения.

Руководство по реализации

Необходимо рассмотреть следующие правила:

a) оборудование, информацию или программное обеспечение нельзя выносить без предварительного разрешения;
b) работники, подрядчики и пользователи третьей стороны, имеющие разрешение на вынос активов, должны быть чётко идентифицированы;
c) необходимо установить предельные сроки выноса и проверку возвращаемого оборудования на соответствие;
d) при необходимости оборудование должно регистрироваться при выносе за пределы помещения и при возврате.

Дополнительная информация

Для выявления несанкционированных записывающих устройств, оружия и т.д. и предотвращения их проноса в помещение организации можно использовать выборочные проверки, обычно применяющиеся для обнаружения несанкционированного выноса имущества. Такие выборочные проверки должны проводиться в соответствии с действующими правовыми нормами и правилами. Персонал должен быть осведомлён о проведении проверок, которые должны быть санкционированы в соответствии с юридическими требованиями.

10 Управление средствами связи и операциями

10.1 Процедуры эксплуатации и обязанности

Цель: обеспечение уверенности в надлежащем и безопасном функционировании средств обработки информации.

Должны быть установлены обязанности и процедуры в отношении управления и функционирования всех средств обработки информации. Они должны включать разработку соответствующих процедур реагирования на инциденты.

С целью минимизации риска неправильного использования систем вследствие небрежности или злого умысла, следует, по возможности, реализовывать принцип разделения полномочий.

10.1.1 Документальное оформление операционных процедур

Определение

Процедуры эксплуатации должны документироваться, сохраняться и быть доступным и для всех пользователей, которым они понадобятся.

Руководство по реализации

Документированные процедуры должны быть разработаны в отношении обслуживания систем обработки и обмена информацией, в частности процедуры запуска и безопасного завершения работы компьютеров (серверов), процедуры резервирования, текущего обслуживания и ремонта оборудования, обеспечения надлежащей безопасности помещений с компьютерным и коммуникационным оборудованием.

Процедуры эксплуатации должны определять инструкции по детальному выполнению каждого задания, включая:

a) обработку и управление информацией;
b) дублирование (см. 10.5);
c) определение требований в отношении графика заданий, включающие взаимозависимости между системами; время начала выполнения самого раннего задания и время завершения самого последнего задания;
d) обработку ошибок или других исключительных ситуаций, которые могли бы возникнуть в течение выполнения заданий, включая ограничения на использование системных утилит (см. 11.5.4);
e) необходимые контакты на случай неожиданных операционных или технических проблем;
f) специальные мероприятия по управлению выводом данных, например, использование специальной бумаги для печатающих устройств или особых процедур применительно к выводу конфиденциальной информации, включая процедуры для безопасной утилизации выходных данных незавершенных нормально заданий (см. 10.7.2 и 10.7.3);
g) процедуры перезапуска и восстановления системы при возникновении системных сбоев;
h) управление информацией системного и контрольного журналов (см. 10.10).

С процедурами эксплуатации и документированными процедурами действий системы надо обращаться как с официальными документами и изменения в них должны санкционироваться руководством организации. Там, где это технически осуществимо, информационные системы должны находиться под непрерывным управлением с использованием таких же процедур, инструментов и средств.

10.1.2 Управление изменениями

Определение

Изменения в средствах обработки информации и системах должны находиться под контролем.

Руководство по реализации

Операционные системы и прикладное программное обеспечение и изменения в них должны быть предметом жёсткого административного управления.

В частности необходимо рассматривать следующие вопросы:

a) определение и регистрация существенных изменений;
b) планирование и тестирование изменений;

c) оценка возможных последствий таких изменений;
d) формализованная процедура утверждения предлагаемых изменений;
e) подробное информирование об изменениях всех заинтересованных лиц;
f) процедуры по нейтрализации неисправностей, включая процедуры и обязанности по аварийному окончанию и восстановлению неудачных изменений и непредвиденных событий.

С целью обеспечения удовлетворительного контроля за всеми изменениями в оборудовании, программном обеспечении или процедурах должны быть в наличии формализованные административные ответственности и процедуры. При осуществлении изменений вся соответствующая информация должна сохраняться в контрольном журнале.

Дополнительная информация

Неадекватный контроль за изменениями в системах и средствах обработки информации является общераспространённой причиной отказов в системах или сбоях в процессе обеспечения безопасности. Изменения операционной среды, особенно при переводе системы из этапа опытно-конструкторских работ на эксплуатационный этап, могут повлиять на надёжность приложений (см. также 12.5.1)

Изменения в операционной системе надо вводить только при наличии веской причины для бизнеса, такой как возрастание риска для системы. Обновление систем с помощью самых последних опций операционных систем и прикладных программ не всегда соответствует интересам бизнеса, потому что это может привести к увеличению уязвимостей и усилению нестабильности, чем применение действующего варианта. Может также возникнуть необходимость в дополнительном обучении, расход на лицензии, поддержке, обслуживании, и нового технического обеспечения, особенно во время переходного периода.

10.1.3. Разделение обязанностей

Определение

Для уменьшения возможностей несанкционированного или ненамеренного изменения или неправильного использования активов организации обязанности и сферы ответственности должны быть разделены.

Руководство по реализации

Разделение обязанностей является методом снижения риска случайного или намеренного неправильного использования системы. Необходимо заботиться о том, чтобы ни один человек не мог получить доступа к активам, модифицировать или использовать их без разрешения или, не будучи обнаруженным. При создании средств контроля необходимо учитывать возможность тайного сговора.

Для небольших организаций эти мероприятия труднодостижимы, однако данный принцип должен быть применен насколько это возможно и реально. В случаях, когда разделение обязанностей осуществить затруднительно, следует рассматривать использование других мероприятий по управлению информационной безопасностью, таких как мониторинг деятельности, использование журналов аудита, а также мер административного контроля. В то же время важно, чтобы аудит безопасности оставался независимой функцией.

10.1.4 Разделение опытно-конструкторского оборудования, испытательного и эксплуатационного оборудования

Определение

Опытно-конструкторское, испытательное и эксплуатационное оборудование должно быть разделено в целях снижения рисков несанкционированного доступа или изменений в операционной системе.

Руководство по реализации

Следует идентифицировать уровень разделения эксплуатационной среды, испытательной и опытно-конструкторской, который необходим для предотвращения проблем, и внедрить соответствующие меры контроля.

Необходимо рассмотреть следующие вопросы:

a) должны быть определены и документированы правила перевода программного обеспечения из статуса разработки в статус эксплуатации;
b) программное обеспечение для разработки и эксплуатации должно работать на различных системах или компьютерных процессорах (серверах), и в различных доменах или директориях;
c) компиляторы, редакторы и другие инструментальные средства разработки или системные утилиты не должны быть доступны в операционной среде без крайней необходимости;
d) среда испытательной системы должна как можно более точно имитировать среду операционной системы;
e) пользователи должны применять различные профили для операционных и испытательных систем, а меню должны отображать соответствующие идентифицирующие сообщения для снижения риска ошибки;
f) секретные данные не должны копироваться в среду испытательных систем (см. 12.4.2).

Деятельность, связанная с разработкой и тестированием может быть причиной серьезных проблем, например, нежелательные изменения файлов или системной среды, а также системные сбои. В этом случае необходимо поддерживать состояние отдельной среды, в которой следует выполнять комплексное тестирование с известной стабильностью и предотвращать несанкционированный доступ со стороны разработчиков.

Там, где сотрудники, отвечающие за разработку и тестирование, имеют доступ к системе и данным среды промышленной эксплуатации, они имеют возможность установить несанкционированную и непроверенную программу или изменить данные в операционной среде. В некоторых системах этой возможностью можно злоупотребить для совершения мошенничества или введения непроверенного или враждебного кода, что может создать серьёзные проблемы при эксплуатации.

Разработчики и специалисты, проводящие тестирование, могут также быть причиной угроз безопасности операционной информации. Если разработка и тестирование производятся в одной компьютерной среде, это может стать причиной непреднамеренных изменений программного обеспечения и информации. Разделение сред разработки, тестирования и эксплуатации является, следовательно, целесообразным для уменьшения риска случайного изменения или неавторизованного доступа к программному обеспечению и бизнес данным среды промышленной эксплуатации (см. также 12.4.2 для защиты тестовых данных).

10.2 Управление поставкой услуг третьей стороной

Цель: Реализация и сохранение соответствующего уровня информационной безопасности и поставки услуг согласно договорам о поставке услуг третьей стороной.

Организация должна проверять реализацию соглашений, контролировать соответствие соглашениям и управлять изменениями для обеспечения того, чтобы поставляемые услуги удовлетворяли всем требованиям, согласованным с третьей стороной.

10.2.1 Поставка услуг

Определение

Необходимо обеспечить реализацию, эксплуатацию и обслуживание третьей сторо-

ной средств контроля безопасности, определений услуг и уровней поставок, включённых в соглашение о поставках услуг третьей стороной.

Руководство по реализации

Поставка услуг третьей стороной должна включать согласованные меры по обеспечению безопасности, определения услуг и аспекты обеспечения обслуживания. В случае проведения мероприятий аутсорсинга, организация должна планировать необходимое перемещение (информации, средств обработки информации и всего, что надо переделать) и должна обеспечить безопасность во время перемещения.

Организация должна обеспечить поддержание третьей стороной достаточного потенциала услуг наряду с реальными планами, предназначенными для гарантирования уровней непрерывности поставки услуг в случае серьёзных сбоев в оказании услуг или каких-либо бедствий (см. 14.1).

10.2.2 Мониторинг и пересмотр услуг третьей стороны

Определение

Услуги, отчёты и записи, предоставляемые третьей стороной, должны подвергаться регулярному мониторингу и пересмотру, а также регулярному аудиту.

Руководство по реализации

Мониторинг и пересмотр услуг третьей стороны призваны обеспечить соблюдение условий соглашений, касающихся информационной безопасности и должное управление инцидентами и проблемами информационной безопасности. Это должно включать отношения в процессе управления услугами и процесс между организацией и третьей стороной для:

a) мониторинга уровней производительности услуг с целью проверки соблюдения условий соглашений;
b) пересмотра отчётов об услугах, предоставляемых третьей стороной, и организация совещаний по результатам работы, как оговорено в соглашениях;
c) обеспечения информации об инцидентах безопасности и пересмотр этой информации третьей стороной и организацией, как это предусмотрено соглашениями и всеми вспомогательными руководствами и процедурами;
d) пересмотра контрольных журналов и записей об инцидентах безопасности третьей стороны, проблемах в ходе эксплуатации, отказах, отслеживании неисправностей и нарушений, связанных с поставленными услугами;
e) решения и устранения любых выявленных проблем.

Ответственность за управление отношениями с третьей стороной должны быть возложены на определённое лицо или группу управления услуг. Кроме того, организация должна обеспечить распределение обязанностей третьей стороны по проверке соответствия требованиям соглашений и их реализации. Для мониторинга соответствия требованиям соглашений (см. 6.2.3), в особенности требованиям информационной безопасности должно быть достаточно технических навыков и ресурсов. При обнаружении недостатков в процессе поставки услуг необходимо предпринять соответствующие действия.

Организация должна поддерживать необходимый общий контроль и наблюдение за всеми аспектами доступа и обработки секретной или критической информации или средств обработки информации третьей стороной. Организация должна следить за всеми действиями, относящимися к безопасности, такими как управление внесением изменений, идентификация уязвимостей и сообщения об инцидентах информационной безопасности и ответные действия, посредством чётко определённого процесса отчётности, формата и структуры.

Дополнительная информация

В случае заключения договора с внешними фирмами организация должна быть ос-

ведомлена о том, что организация несёт всю ответственность за информацию, обрабатываемую этими внешними фирмами.

10.2.3 Управление внесением изменений в услуги третьей стороны

Определение

Внесение изменений в предоставление услуг, включая поддержание и улучшение существующих политик информационной безопасности, процедур мер контроля должно управляться с учётом критичности задействованных экономических систем и процессов и переоценки рисков.

Руководство по реализации

В процессе управления внесением изменений в услуги третьей стороны необходимо учитывать:

a) изменения, осуществляемые организацией для реализации:
   1) улучшения предлагаемых текущих услуг;
   2) разработки любых новых прикладных программ и систем;
   3) модификаций или обновлений политик и процедур организации;
   4) нового контроля по результатам решения инцидентов в информационной безопасности и при усовершенствованиях безопасности.
b) изменения в услугах третьей стороны для реализации:
   1) изменений и улучшения сетей;
   2) использования новых технологий;
   3) принятия новой продукции или более новых опций/выпусков;
   4) новых инструментальных средств и среды разработки;
   5) изменения в физическом месторасположении средств обслуживания;
   6) смены продавцов (оптовых фирм).

10.3 Планирование нагрузки и приемка систем

Цель: сведение к минимуму риска сбоев в работе систем.

Для обеспечения доступности данных, требуемых производительности и ресурсов систем необходимы предварительное планирование и подготовка.

Для снижения риска их перегрузки систем необходимо проведение анализа предполагаемой нагрузки.

Требования к эксплуатации новых систем должны быть определены, документально оформлены и протестированы перед их приемкой и использованием.

10.3.1 Управление производительностью

Определение

Использование ресурсов должно контролироваться и быть отлаженным, а также должен быть сделан прогноз будущей требуемой производительности.

Руководство по реализации

Для каждого нового и текущего вида деятельности должны быть определены требования к производительности. Для обеспечения и, если необходимо, улучшения доступности и эффективности систем должны применяться настройка и мониторинг систем. Для своевременного указания проблем должны быть в наличии средства обнаружения. При прогнозировании будущих требований к производительности необходимо принимать во внимание новые требования к бизнесу и системам, а также текущие и прогнозируемые тенденции в усилении возможностей обработки информации организации.

Особое внимание надо уделить любым ресурсам с продолжительным временем реа-

лизации (подготовки) поставки и высокой стоимостью; следовательно, руководители должны контролировать ключевые системные ресурсы. Они должны определять тенденции в использовании, особенно по отношению к бизнес-приложениям или средствам и методам управления информационными системами.

Руководители должны использовать эту информацию для выявления избежания узких потенциальных мест и зависимости от ведущих специалистов, что может представить угрозу безопасности системы или услугам, и планировать соответствующие меры.

10.3.2 Приёмка систем

Определение

Должны быть установлены критерии приёмки новых информационных систем, обновлений, и новых версий и должны проводиться подходящие испытания систем(ы) во время разработки и до приёмки.

Руководство по реализации

Менеджеры должны гарантировать, что требования и критерии приёмки новых систем чётко определены, согласованы, документально оформлены и опробованы. Новые информационные системы, обновления и новые версии должны переходить на стадию производства только после получения официальной приёмки. Перед официальной приёмкой необходимо рассмотреть следующие факторы:

a) оценка выполнения требований к мощности и производительности компьютера;
b) определение процедур восстановления после сбоев и повторного запуска и планы обеспечения непрерывной работы;
c) подготовка и тестирование типовых операционных процессов на соответствие определенным стандартам;
d) наличие необходимого набора средств контроля информационной безопасности;
e) разработка эффективных руководств по процедурам;
f) мероприятия по обеспечению непрерывности бизнеса, в соответствие с требованиями 14.1;
g) обязательная проверка отсутствия неблагоприятного влияния новых систем на существующие, особенно во время максимальных нагрузок, например в конце месяца;
h) контроль проведения анализа влияния, оказываемого новой системой на общую информационную безопасность организации;
i) организация профессиональной подготовки персонала к эксплуатации и использованию новых систем;
j) удобство использования, насколько это влияет на производительность пользователя и помогает избежать субъективной ошибки.

Для консультирования на всех стадиях процесса разработки новых систем должны привлекаться службы поддержки и пользователи, с целью обеспечения эффективной эксплуатации проектируемой системы. Соответствующие тесты должны проводиться для подтверждения того, что все критерии приемки удовлетворены полностью.

Дополнительная информация

Приёмка может включать официальный процесс сертифицирования и аккредитации для проверки на соответствие требованиям безопасности.

10.4 Защита от вредоносного и подвижного кода

Цель: обеспечение защиты целостности подвижного кода и массивов информации.

Необходимо принимать меры предотвращения и обнаружения внедрения вредоносного кода и несанкционированного подвижного кода.

Программное обеспечение и средства обработки информации уязвимы к внедрению вредоносного кода, такого как компьютерные вирусы, сетевые "черви", "троянские кони" и логические бомбы. Пользователи должны быть осведомлены об опасности использования неавторизованного или вредоносного кода. Соответствующие руководители должны обеспечить внедрение специальных средств контроля с целью предотвращения, обнаружения и удаления вредоносного кода и подвижного кода проникновения подобных программ.

10.4.1 Мероприятия по управлению информационной безопасностью для борьбы с вредоносным программным обеспечением

Определение

С целью обнаружения и предотвращения проникновения вредоносного кода, необходимы планирование и реализация мероприятий по управлению информационной безопасностью, а также процедур, обеспечивающих соответствующую осведомленность пользователей.

Руководство по реализации

Защита от вредоносного кода должна основываться на программном обеспечении по обнаружению вредоносного кода, понимании требований безопасности, соответствующих мерах контроля доступа к системам и надлежащего управления изменениями. Необходимо рассматривать следующие мероприятия по управлению информационной безопасностью:

a) создание документированной политики, требующей соблюдения лицензионных соглашений и устанавливающей запрет на использование несанкционированного программного обеспечения (см. 15.1.2);
b) создание документированной политики защиты от рисков, связанных с получением файлов и программного обеспечения либо из внешних сетей, либо через внешние сети, или из любой другой среды. В этой политике должно содержаться указание о необходимости принятия защитных мер;
c) проведение регулярных инвентаризаций программного обеспечения и данных систем, поддерживающих критические бизнес-процессы. Необходима формализованная процедура по расследованию причины появления любых неавторизованных или измененных файлов в системе;
d) установку и регулярное обновление антивирусного программного обеспечения для обнаружения и сканирования компьютеров и носителей информации, запускаемого в случае необходимости в качестве превентивной меры или как рутинная процедура, проверки должны включать:
   1) проверку всех файлов на электронных или оптических носителях информации, и файлов, полученных из сетей, на наличие вредоносного кода перед работой с этими файлами;
   2) проверку любых вложений электронной почты и скачиваемой информации на наличие вредоносного программного обеспечения до их использования, эта проверка может быть выполнена в разных точках, например, на серверах электронном почты, персональных компьютерах или при входе в сеть организации;
   3) проверку web-страниц на наличие вредоносного кода;
e) определение управленческих процедур и обязанностей, связанных с защитой от вредоносного кода, обучения применению этих процедур, а также вопросов оповещения и восстановления после атак вредоносного кода (см. 13.1 и 13.2);
f) подготовка соответствующих планов по обеспечению непрерывности бизнеса в

части восстановления после вирусных атак, включая все необходимые мероприятия по резервированию и восстановлению данных и программного обеспечения (см. раздел 14);

g) реализация процедур регулярного сбора такой информации, как подписка на список адресатов и/или проверку web-сайтов, предоставляющую информацию о новом вредоносном коде;

h) реализация процедур по контролю всей информации, касающейся вредоносного кода, обеспечение точности и информативности предупредительных сообщений, для определения различия между ложными и реальными вирусами должны использоваться профессиональные источники, например, респектабельные журналы, заслуживающие доверия интернет-сайты или поставщики антивирусного программного обеспечения, все пользователи должны быть осведомлены о проблеме ложных вирусов и действиях при их получении.

Дополнительная информация

Использование двух или более программных изделий, защищающих от вредоносного кода в среде обработки информации от различных продавцов, может улучшить эффективность защиты от вредоносного кода.

Для обеспечения автоматических корректировок файлов определения можно установить программное обеспечение защиты от вредоносного кода, а также для обеспечения защиты существуют современные сканирующие машины. Для проведения автоматических проверок на каждом рабочем столе можно установить это программное обеспечение.

Для защиты от внедрения вредоносного кода во время обслуживания и проведения чрезвычайных процедур, которые могут привести к блокированию средств защиты от вредоносного кода, необходимо соблюдать осторожность.

10.4.2 Средства защиты от подвижного кода

Определение

При наличии санкционированного подвижного кода конфигурация должна обеспечить функционирование санкционированного подвижного кода в соответствии с чётко определённой политикой безопасности, а подвижный несанкционированный код должен быть защищён от реализации

Руководство по реализации

Для защиты от подвижного кода, выполняющего несанкционированные действия, необходимо рассмотреть следующие меры:

a) реализацию подвижного кода в логически изолированной среде;

b) блокирование использования подвижного кода;

c) блокирование приёма подвижного кода;

d) задействование технических мер, предусмотренных в специальных системах, для обеспечения управления подвижным кодом;

e) контроль за ресурсами, доступными для подвижного кода;

f) криптографические средства контроля для определения подлинности подвижного кода.

Дополнительная информация

Подвижный код является кодом программного обеспечения, который переходит из одного компьютера в другой, затем автоматически реализуется и выполняет специфическую функцию с незначительным участием пользователя или вообще без него. Подвижный код связан с несколькими промежуточными программными обеспечениями.

Кроме обеспечения отсутствия вредоносного кода в подвижном коде, контроль за подвижным кодом важен для избежания несанкционированного использования или разрушения системы, сети или прикладных ресурсов и других нарушений информационной

безопасности.

10.5 Дублирование

Цель: Поддержание целостности и доступности информации и средств обработки информации.

Для реализации согласованной политики и стратегии (см. также 14.1) по снятию дублирующих копий данных и имитирования их своевременного восстановления необходимо выработать регулярные процедуры.

10.5.1 Дублирование информации

Определение

Дублирующие копии информации и программного обеспечения должны осуществляться и проверяться на регулярной основе в соответствии с согласованной политикой дублирования.

Руководство по реализации

Для восстановления всей значимой информации и программного обеспечения после какого-либо бедствия или отказа в работе носителей данных должны быть предусмотрены адекватные средства дублирования.

Для дублирования информации необходимо рассмотреть следующие меры:

a) следует определить необходимый уровень дублирующей информации;
b) необходимо получить точные и завершённые отчёты о дублирующих копиях и документированных процедурах восстановления;
c) степень (полное и дифференцированное дублирование) и частота дублирований должны отражать бизнес-требования организации, включая требования безопасности информации, и критичность информации для обеспечения бесперебойной работы организации;
d) копии должны храниться в удалённом месте на значительном расстоянии для избежания повреждений вследствие какого-либо бедствия в основном здании;
e) резервная информация должна быть обеспечена уровнем физической защиты и защиты от воздействий окружающей среды (раздел 9), в соответствии с уровнем безопасности в основном здании. Мероприятия, применяемые к оборудованию в основном здании, должны распространяться на резервный пункт;
f) резервное оборудование должно регулярно подвергаться тестированию, для обеспечения уверенности в том, в случае чрезвычайных ситуаций, на его работу можно положиться;
g) процедуры восстановления следует регулярно актуализировать и тестировать, для обеспечения уверенности в их эффективности, а также в том что для выполнения этих процедур потребуется не больше времени, чем определенно операционными процедурами восстановления;
h) в условиях конфиденциальности копии должны шифроваться.

Мероприятия по дублированию для отдельных систем должны регулярно тестироваться для обеспечения соответствия требованиям планов непрерывности деловой деятельности (см. раздел 14). Для критических систем мероприятия по дублированию должны охватывать информацию приложений и данных всех систем, необходимых для восстановления полной системы в случае какого-либо бедствия.

Следует определять периоды хранения важной служебной информации, а также учитывать требования к архивным копиям долговременного хранения (см. 15.1.3).

Дополнительная информация

Для облегчения процесса дублирования и восстановления мероприятия по дублиро-

ванию можно автоматизировать. Такие автоматизированные варианты должны серьёзно тестироваться перед реализацией и на регулярной основе после неё.

10.6 Управление безопасностью сетей

Цель: Обеспечение защиты информации в сетях и поддерживающей инфраструктуры.

Управление безопасностью сетей, которые могут выходить за пределы границ организации, нуждается в тщательном рассмотрении потока данных, юридических выводов, мониторинге и защите.

Для защиты секретной информации, проходящей по общедоступным сетям, могут потребоваться дополнительные меры.

10.6.1 Средства контроля сетей

Определение

Сети должны адекватно управляться и контролироваться с целью защиты от угроз и поддержания безопасности систем и приложений с помощью систем, включая информацию.

Руководство по реализации

Руководители, отвечающие за поддержку сетевых ресурсов должны обеспечивать внедрение средств контроля безопасности данных в сетях и защиту подключенных сервисов от неавторизованного доступа. В частности, необходимо рассмотреть следующие меры и средства управления информационной безопасностью:

a) следует распределять ответственность за поддержание сетевых ресурсов и за поддержание компьютерных операций (см. 10.1.3);
b) следует устанавливать процедуры и обязанности по управлению удаленным оборудованием, включая оборудование, установленное у конечных пользователей;
c) если необходимо, специальные средства контроля следует внедрять для обеспечения конфиденциальности и целостности данных, проходящих по общедоступным сетям или по беспроводным сетям, а также для защиты подключенных систем (11.4 и 12.3). Могут также потребоваться специальные средства контроля для поддержания доступности сетевых сервисов и рабочих станций;
d) для обеспечения фиксирования действий, связанных с безопасностью, должны применяться соответствующая регистрация и мониторинг;
e) действия по управлению необходимо тщательно соизмерять как с требованиями к сервисам от бизнеса, так и с общими требованиями к обеспечению безопасности инфраструктуры обработки информации.

Дополнительная информация

Дополнительную информацию по безопасности сетей можно найти в стандарте [8].

10.6.2 Безопасность сетевых услуг

Определение

Возможности и уровни безопасности, и административные требования всех сетевых сервисов должны быть определены и включены во все соглашения по сетевым сервисам, независимо от того, предоставляются ли эти услуги для внутреннего пользования или вне пределов организации.

Руководство по реализации

Способность поставщика сетевых сервисов управлять согласованными сервисами безопасным путём должна быть определена и контролироваться на регулярной основе, а

право на аудит должно быть согласовано.

Необходимо определить меры по обеспечению безопасности, обязательные для таких определённых сервисов, как возможности безопасности, уровни безопасности и административные требования. Организация должна требовать от поставщиков сервисов реализации этих мер.

Дополнительная информация

Сетевые сервисы включают предоставление соединений, сервисы частных сетей, и решение проблем с безопасностью управляемых сетей с дополнительными услугами (таких как: брандмауэры и системы обнаружения вторжений). Эти услуги могут варьироваться от неуправляемых полос пропускания до сложных дополнительных предложений.

Возможностям безопасности сетевых услуг могут быть:

a) технология, применяемая для защиты сетевых услуг, таких как аутентификация, шифрование и средства контроля соединений сетей;
b) технические параметры, требуемые для безопасного соединения с сетевыми услугами в соответствии с правилами безопасности и соединения сетей;
c) процедуры применения сетевых услуг для ограничения доступа к сетевым услугам или приложениям, где это необходимо.

10.7 Манипулирование носителями информации

Цель: Предотвращение несанкционированного разглашения, модифицирования, удаления или разрушения актива и прерывания деловой деятельности.

Носители должны контролироваться и быть защищены.

Необходимо выработать соответствующие рабочие процедуры по защите документов, компьютерных носителей (например, лент, дисков), данных входов/выходов и системной документации от несанкционированного разглашения, модифицирования, удаления и разрушения.

10.7.1 Управление съёмными носителями

Определение

Для управления съёмными носителями должны существовать некоторые процедуры.

Руководство по реализации

Для управления съёмными носителями необходимо рассмотреть следующие правила:

a) если носители информации многократного использования больше не требуются и удаляются за пределы организации, их содержимое должно стать невосстанавливаемым;
b) где это необходимо и целесообразно, в отношении всех уничтожаемых носителей информации должно быть принято соответствующее решение, а также сделана запись в регистрационном журнале, который должен храниться;
c) все носители информации должны храниться в надежном, безопасном месте, в соответствии с требованиями изготовителей;
d) информация, хранящаяся на носителях, в которой нуждаются дольше, чем срок службы носителя (в соответствии со спецификациями изготовителя) должна также находиться в другом месте для избежания утери информации вследствие изношенности носителя;
e) для ограничения вероятности потери данных должна предусматриваться регистрация съёмных носителей;
f) съёмные дисководы должны задействоваться только, если для этого есть серьёзная причина.

Все процедуры и уровни санкционирования должны быть чётко определены.

Дополнительная информация

Съёмные носители информации включают ленты, диски, флэш-диски, жёсткие диски, CD, DVD и печатные носители.

10.7.2 Ликвидация носителей информации

Определение

Носители должны ликвидироваться надёжным безопасным образом, если в них больше нет необходимости, посредством формализованных процедур.

Руководство по реализации

Формальные процедуры безопасной ликвидации носителей информации призваны свести к минимуму риск утечки секретной информации несанкционированным лицам. Процедуры безопасной ликвидации носителей, содержащих секретную информацию, должны соответствовать степени секретности этой информации. Необходимо рассмотреть следующие пункты:

a) носители, содержащие важную информацию, следует хранить и ликвидировать надежно и безопасно (например, посредством сжигания/ измельчения); если носители планируются использовать в пределах организации для других задач, информация на них должна быть уничтожена;
b) для определения объектов, которые могут потребовать безопасной ликвидации, должны быть специальные процедуры;
c) может оказаться проще принимать меры безопасной ликвидации в отношении всех носителей информации, чем пытаться сортировать носители по степени важности;
d) многие организации предлагают услуги по сбору и ликвидации бумаги, оборудования и носителей информации. Следует тщательно выбирать подходящего подрядчика с учетом имеющегося у него опыта и обеспечения необходимого уровня информационной безопасности;
e) по возможности следует регистрировать ликвидацию важных объектов с целью последующего аудита.

При сборе носителей информации для ликвидации необходимо учитывать эффект агрегации, который может вызвать превращение большого объёма несекретной информации в секретную.

Дополнительная информация

Критичная информация может быть восстановлена при небрежной ликвидации носителей (см. также в 9.2.6 информацию о ликвидации оборудования).

10.7.3 Процедуры обработки информации

Определение

С целью обеспечения защиты информации от неавторизованного раскрытия или неправильного использования, необходимо определить процедуры обработки и хранения информации.

Руководство по реализации

Эти процедуры должны быть разработаны для обработки, хранения и передачи информации с учетом классификации информации (см. 7.2). Необходимо предусмотреть следующие меры:

a) обработка и маркирование всех носителей информации должна соответствовать указанному уровню секретности;
b) ограничение доступа с целью идентификации несанкционированного персонала;

c) обеспечение формализованной регистрации авторизованных получателей данных;
d) обеспечение уверенности в том, что данные ввода являются полными, что процесс обработки завершается должным образом, и что имеется подтверждение вывода данных;
e) обеспечение защиты информации, находящейся в буфере данных и ожидающей вывода, должно соответствовать важности этой информации;
f) хранение носителей информации в соответствии с требованиями изготовителей;
g) сдерживать распространение данных до минимума;
h) четкая маркировка всех копий данных, предлагаемых вниманию авторизованного получателя;
i) регулярный пересмотр списков рассылки и списков авторизованных получателей.

Дополнительная информация

Эти процедуры касаются информации, содержащейся в документах, вычислительных системах, сетях, переносных компьютерах, почте, автоответчиках, речевой связи вообще, мультимедийных средствах, почтовой службе, использования факсов и других секретных объектах, например, банковских чеках, счётах-фактурах.

10.7.4 Безопасность системной документации

Определение

Системная документация должна быть защищена от несанкционированного доступа.

Руководство по реализации

Для защиты системной документации необходимо рассмотреть следующие меры:

a) системную документацию следует хранить безопасным образом;
b) список лиц, имеющих доступ к системной документации, следует сводить к минимуму; доступ должен быть санкционирован владельцем бизнес-приложения;
c) системную документацию, полученную/поддерживаемую через общедоступную сеть, следует защищать надлежащим образом.

Дополнительная информация

Системная документация может содержать определённую секретную информацию, например, описания прикладных процессов, процедур, структур данных, процессов санкционирования.

10.8 Обмен информацией

Цель: поддержание информации и программного обеспечения, обмен которыми происходит как внутри организации, так и с другими организациями.

Обмен информацией и программным обеспечением между организациями должен основываться на формальной политике обмена, осуществляемой в соответствии с соглашениями об обмене и не должна противоречить какому-либо релевантному законодательству (см. раздел 15).

Необходимо установить процедуры и стандарты для защиты информации и физических носителей, содержащих пересылаемую информацию.

10.8.1 Политики и процедуры обмена информацией

Определение

Должны быть в наличии политики, процедуры и средства контроля для защиты об-

мена информацией посредством использования всех типов средств связи.

Руководство по реализации

Процедуры и средства контроля, задействованные при использовании электронных средств связи для обмена информацией, должны включать:

a) процедуры, предназначенные для защиты обмененной информации от перехвата, копирования, модифицирования, направления по неправильному маршруту и разрушения;
b) процедуры обнаружения вредоносного кода, который может передаваться с помощью электронных средств связи, и защиты от него (см. 10.4.1);
c) процедуры защиты переданной секретной электронной информации, которая имеет вид дополнения;
d) политику или правила, определяющие приемлемое использование электронных средств связи (см.7.1.3);
e) процедуры применения беспроводной связи с учётом возможных рисков;
f) обязательства работника, подрядчика или какого-либо другого пользователя не создавать опасности для организации, например, посредством диффамации, причинением беспокойства, персонацией, рассылкой писем по нескольким адресам с тем, чтобы получатель разослал их по другим адресам, несанкционированной закупки, и т.д.;
g) применение шифровальных технологий, например, для защиты конфиденциальности, целостности и аутентичности информации (см. 12.3);
h) руководства по хранению и утилизации всей деловой корреспонденции, включая сообщения в соответствии с релевантными национальным и региональным законодательством;
i) неоставление секретной или критической информации в печатном оборудовании, например, в копировальном оборудовании, принтерах и факсах, так как к ним может получить доступ несанкционированный персонал;
j) средства контроля и ограничения, связанные с отправлением средств связи, например, автоматическое отправление электронной почты по внешним почтовым адресам;
k) напоминание сотрудникам о необходимости принятия соответствующих мер предосторожности, например, чтобы избежать подслушивания или перехвата информации при использовании телефонной связи:
   1) лицами, находящимися в непосредственной близости, особенно при пользовании мобильными телефонами;
   2) прослушивания телефонных переговоров путем физического доступа к трубке или телефонной линии;
   3) посторонними лицами со стороны адресата;
l) не оставлять сообщений, содержащих секретную информацию на автоответчиках, переадресация на которых произошла вследствие ошибки соединения или автоответчиков операторов связи, поскольку эти сообщения могут быть воспроизведены неавторизованными лицами;
m) напоминание сотрудникам о возможных рисках, присущих использованию факсимильных аппаратов, а именно:
   1) неавторизованный доступ к встроенной памяти для поиска сообщений;
   2) преднамеренное или случайное перепрограммирование аппаратов с целью передачи сообщений по определенным номерам;
   3) отсылка документов и сообщений по неправильному номеру вследствие неправильного набора, либо из-за использования неправильно сохраненного номера.
n) напоминание персоналу не регистрировать демографические данные, такие как

адрес электронной почты или другой личной информации, в программном обеспечении во избежание их сбора для несанкционированного использования;

o) напоминание персоналу о том, что факсы и фотокопировальные устройства имеют страничные кэши и сохраняют страницы в случае сбоев при подаче бумаги или передачи, и эти страницы печатаются после устранения неисправности.

Кроме того, персоналу надо напоминать о недопустимости ведения конфиденциальных разговоров в общественных местах или офисах с открытыми окнами и помещениях без звукоизоляции.

Средства обмена информацией должны соответствовать любым релевантным правовым требованиям (см. раздел 15).

Дополнительная информация

Обмен информацией может происходить посредством различных носителей информации, включая откачку из Интернета и получение информации от продавцов, торгующих серийной продукцией.

Необходимо учитывать правовые последствия и последствия для бизнеса и безопасности, связанные с обменом электронными данными, электронной торговлей, электронными средствами связи и требованиями к средствам контроля.

Информация может подвергаться опасности из-за недостаточной осведомленности сотрудников по использованию средств передачи информации. В частности, информация может быть подслушана при переговорах по мобильному телефону в общественном месте, а также с автоответчиков, неправильно направлено сообщение по электронной почте, информация может также быть скомпрометированной вследствие неавторизованного доступа к системе голосовой почты, или случайной отсылки факсимильных сообщений неправильному адресату.

Бизнес-операции могут быть нарушены, и информация может быть скомпрометирована, в случае отказа, перегрузки или прерывания в работе средств взаимодействия (см. 10.3 и раздел 14). Информация может быть также скомпрометирована, если к ней имел место доступ несанкционированных пользователей (раздел 11).

10.8.2 Соглашения по обмену информацией

Определение

Между организацией и внешними сторонами необходимо выработать соглашения по обмену информацией и программным обеспечением.

Руководство по реализации

Соглашения по обмену должны предусматривать следующие условия:

a) обязанности руководства по контролю и уведомлению о передаче, отправке и получении;
b) процедуры для уведомления отправителя о передаче, отправке и получении;
c) процедуры прослеживаемости и невозможности отказа от своих обязательств;
d) минимальные технические требования по формированию и передаче пакетов данных;
e) соглашения по условному депонированию;
f) требования к курьерской службе;
g) ответственность и обязательства в случае потери данных;
h) использование согласованной системы маркировки для важной или критичной информации, обеспечивающей уверенность в том, что значение этой маркировки будет сразу же понято и информация будет соответственно защищена;
i) определение владельцев, а также обязанностей по защите данных, учет авторских прав на программное обеспечение, и аналогичных вопросов (15.1.2 и

15.1.4);

j) технические требования в отношении записи и считывания информации и программного обеспечения;

k) любые специальные средства контроля, которые могут потребоваться для защиты важных объектов, например криптографические ключи (см.12.3).

Необходимо выработать и поддерживать политики, процедуры и стандарты по защите информации и физических носителей информации по пересылке (см. также 10.8.3), и в соглашениях по обмену информацией должны делаться ссылки на эти политики, процедуры и стандарты.

Часть соглашения, касающаяся безопасности, должна отражать степень секретности задействованной деловой информации.

Дополнительная информация

Соглашения могут быть в электронном виде или написанные от руки и могут принимать вид формального договора или условий трудового соглашения. Что касается секретной информации, специфические механизмы, используемые для обмена подобной информацией, должны быть совместимы для всех организаций и типов соглашений.

10.8.3 Переносимые физические носители информации

Определение

Содержащие информацию носители должны быть защищены от несанкционированного доступа, неправильного использования или разрушения во время транспортировки за пределы физических границ организации.

Руководство по реализации

Для защиты носителей информации, переносимых их одного места в другое, необходимо рассмотреть следующие правила:

a) следует использовать надежных перевозчиков или курьеров;

b) список авторизованных курьеров необходимо согласовывать с руководством;

c) следует разработать процедуру проверки идентификации курьеров;

d) упаковка должна быть достаточной для защиты содержимого от любого физического повреждения, которое, может иметь место при транспортировке, и соответствовать требованиям изготовителей носителей информации (например, для программного обеспечения), для примера защиты от любых факторов окружающей среды, которые могут сократить эффективность восстановления среды, такие как тепловое воздействие, влажность или электромагнитные поля;

e) средства контроля следует применять, где это необходимо, для защиты важной информации от неавторизованного раскрытия или модификации. Например:

   1) использование запертых контейнеров;
   2) личная доставка;
   3) использование упаковки, которую нельзя нарушить незаметно (на которой видна любая попытка вскрытия);
   4) в исключительных случаях, разбивку отправления на несколько частей, пересылаемых различными маршрутами.

Дополнительная информация

Информация может быть уязвимой для несанкционированного доступа, неправильного использования или разрушения во время физического перемещения, например, при пересылке носителей по почте или курьером.

10.8.4 Электронный обмен сообщениями

Определение

Информация, участвующая в электронном обмене сообщениями, должна быть

должным образом защищена

Руководство по реализации

Аспекты безопасности при электронном обмене сообщениями должны включать следующее:

a) защита сообщений от несанкционированного доступа, модифицирования или отказа в обслуживании;
b) обеспечение правильной адресации и передачи сообщения;
c) общая надёжность и доступность сервиса;
d) правовые аспекты, например, требования к электронным подписям;
e) получение санкции перед использованием внешних общественных сервисов, таких как мгновенный обмен сообщениями и совместное использование файлов;
f) более жёсткие уровни аутентификации, контролирующие доступ от общественно доступных сетей.

Дополнительная информация

Электронный обмен сообщениями, такой как электронная почта, электронный обмен данными (EDI) и мгновенный обмен сообщениями играют всё более важную роль в деловом обмене информацией. Электронный обмен сообщениями имеет риски, отличные от средств связи, основанные на печатных сообщениях.

10.8.5 Коммерческие информационные системы

Определение

Для защиты информации, связанной с межсоединением систем деловой информации должны быть разработаны и реализованы политики и процедуры.

Руководство по реализации

Аспекты безопасности и последствия соединения таких политик и процедур для бизнеса должны включать:

a) известные уязвимости в административных системах и системах учёта и отчётности, где информация используется совместно с несколькими подразделениями организации;
b) уязвимость информации в офисных системах, связанные, например, с записью телефонных разговоров или переговоров по конференц-связи, конфиденциальностью звонков, хранением факсов, вскрытием и рассылкой почты;
c) учитывать уязвимость информации, предназначенной для совместного использования;
d) исключение использования офисных систем в отношении категорий важной служебной информации и секретных документов, если эти системы не обеспечивают соответствующий уровень защиты (см.7.2);
e) ограничение доступа к данным личных ежедневников отдельных сотрудников, например, работающих на важных проектах;
f) категории сотрудников, подрядчиков или деловых партнеров, которым разрешено использовать систему и рабочие места, с которых может осуществляться к ней доступ (см. 6.2 и 6.3);
g) ограничение определенных возможностей системы для определенных категорий пользователей;
h) идентификация статуса пользователей, например, служащих организации или подрядчиков, в отдельных директориях, для удобства других пользователей;
i) сохранение и резервирование информации, содержащейся в системе (см. 10.5.1);
j) требования по переходу на аварийный режим работы и перечень соответст-

вующих мероприятий (см. раздел 14).

Дополнительная информация

Офисные информационные системы предоставляют благоприятные возможности для более быстрого распространения и совместного использования деловой информации с помощью объединения: документов, компьютеров, передвижной вычислительной техники, мобильных средств связи, почты, речевой почты, речевой связи вообще, почтовой связи и устройств факсимильной связи.

10.9 Сервисы электронной торговли

Цель: Обеспечение защиты сервисов электронной торговли и их безопасное использование.

Необходимо учитывать последствия для безопасности, связанные с применением сервисов электронной торговли, включая: онлайновые операции и требования к средствам контроля. Необходимо также рассмотреть целостность и доступность информации, опубликованной в электронном виде через общественно доступные системы.

10.9.1 Электронная торговля

Определение

Информация, задействованная в электронной торговле, которая проходит через сети общего пользования, должна быть защищена от мошенничества, споров по контракту, несанкционированного разглашения и изменения.

Руководство по реализации

Аспекты безопасности электронной торговли должны включать следующее:

a) уровень достоверности, который каждая сторона требует от заявленной ею своей подлинности, например, посредством аутентификации;
b) процессы санкционирования, связанные с тем, кто может устанавливать цены, выпускать или подписывать ключевую коммерческую документацию;
c) обеспечение полной информированности торговых партнёров об их санкционированиях;
d) определение и выполнение требований конфиденциальности, целостности, доказательство отправки и получения ключевой документации и невозможность отказа от выполнения контрактов, например, связанных с процессами заключения контрактов и подачи заявки на выполнение работ (тендеров);
e) уровень доверия, требуемый для целостности официально объявленных прайслистов;
f) конфиденциальность любых секретных данных или информации;
g) конфиденциальность и целостность любых транзакций с заказами, информации о платежах, подробного адреса доставки и подтверждения о получении;
h) степень определения подлинности по отношению к информации об оплате чеков, предоставляемой заказчиком;
i) выбор наиболее подходящей формы производства платежей для защиты от мошенничества;
j) уровень защиты, необходимый для поддержания конфиденциальности и целостности информации о заказах;
k) избежание потерь или дублирование информации о транзакциях;
l) ответственность, связанная с мошенническими транзакциями;
m) страховые требования.

Многие из вышеупомянутых проблем могут быть решены с использованием криптографических методов, изложенных в 12.3, при этом необходимо обеспечить соответствие

требованиям законодательства (см. 15.1, особенно 15.1.6 относительно законодательства в области криптозащиты).

Соглашения между партнерами в области электронной торговли следует сопровождать документально оформленными договорами, которые устанавливают согласованные между сторонами условия заключения сделок, включая детали авторизации. Могут потребоваться также дополнительные соглашения с поставщиками сетевых и информационных услуг.

Магазины (сети) электронной торговли, ориентированные на массового потребителя, должны обнародовать условия заключения сделок.

Необходимо обеспечивать устойчивость к вирусным атакам на основной сервер электронной торговли, а также предусматривать последствия для безопасности всех сетевых взаимосвязей, при осуществлении электронной торговли (см. 11.4.6).

Дополнительная информация

Электронная торговля уязвима для многих сетевых угроз, которые могут привести к мошеннической деятельности, спорам по контракту и разглашению или модифицированию информации.

В электронной торговле могут использоваться безопасные методы аутентификации, например, применение криптографии с открытым ключом и цифровых подписей (см. также 12.3) для снижения риска. Могут также задействоваться доверенные третьи стороны там, где востребованы подобные сервисы.

10.9.2 Онлайновые транзакции

Определение

Информация, задействованная в онлайновых транзакциях, должна быть защищена для предотвращения неполной передачи, направления по неправильному маршруту, несанкционированного изменения сообщений, несанкционированного разглашения, несанкционированного дублирования сообщений или повторного воспроизведения.

Руководство по реализации

Аспекты безопасности для онлайновых транзакций должны включать следующее:

a) использование электронных подписей каждой из сторон, участвующих в транзакции;
b) все аспекты транзакции, т.е. обеспечение того, что:
   1) мандаты пользователей всех сторон действительны и проверены;
   2) транзакция остаётся конфиденциальной; и
   3) секретность, связанная со всеми сторонами, сохраняется;
c) маршрут связи между всеми тремя участвующими сторонами зашифрован;
d) протоколы, использованные для связи между всеми участвующими сторонами защищены;
e) обеспечение хранения подробностей транзакций за пределами любой общедоступной среды, например, на носителе, имеющемся в Intranet организации, а не на носителе, подверженному прямому доступу из Интернета;
f) там, где используется доверенный орган управления (например, для выпуска и поддержания цифровых подписей и/или цифровых сертификатов), безопасность интегрирована и внедрена во весь сквозной процесс управления сертификат/подпись.

Дополнительная информация

Объём мер защиты должен соответствовать уровню риска, связанного с каждой формой онлайновой транзакции.

Для транзакций может потребоваться соответствие законам, правилам и положениям юрисдикции, на основе которой появились транзакции, обрабатывались, заверялись и

хранились.

Существуют много форм транзакций, которые можно осуществляться в онлайновом режиме, например, договорная, финансовая и т.д.

10.9.3 Общедоступная информация

Определение

Целостность информации с общедоступной системы должна быть защищена от несанкционированного модифицирования.

Руководство по реализации

Программное обеспечение, данные и дополнительную информацию, требующую высокого уровня целостности, доступ к которой осуществляется через системы публичного доступа, необходимо защищать адекватными способами, например, посредством цифровой подписи (см. 12.3.). Системы публичного доступа должны испытываться на слабые места и поломки до того как информация станет общедоступной.

Необходим соответствующий формализованный процесс авторизации прежде, чем информация будет сделана общедоступной. Кроме того, все входные данные должны проверяться и получать одобрение.

Системы, предоставляющие возможность электронной публикации информации, возможность обратной связи и непосредственного ввода информации, должны находиться под надлежащим контролем, с тем, чтобы:

a) полученная информация соответствовала всем законам по защите данных (15.1.4);
b) информация, введенная в систему электронной публикации, обрабатывалась своевременно, полностью и точно;
c) важная информация была защищена в процессе ее сбора, обработки и хранения;
d) доступ к системе электронной публикации исключал бы возможность непреднамеренного доступа к сетям, с которыми она связана.

Дополнительная информация

Информацию системы публичного доступа, например, информацию на Web-сервере, доступную через Интернет, возможно, потребуется привести в соответствие с законодательством и регулирующими нормами страны, под юрисдикцией которых находится система или осуществляется торговля. Несанкционированная модификация опубликованной информации может навредить репутации публикующую организацию.

10.10 Мониторинг

Цель: Обнаружение несанкционированных действий по обработке информации.

Системы должны контролироваться, а события информационной безопасности должны регистрироваться. Для определения проблем информационной системы должны использоваться регистрация дефектов и журналы операторов.

Организация должна соблюдать все правовые требования, применимые к её деятельности по мониторингу и регистрации.

Мониторинг системы должен применяться для проверки эффективности принятых средств контроля и проверки соответствия модели политики доступа.

10.10.1 Регистрация аудита

Определение

Необходимо создать и вести в течение обговоренного периода времени контрольные журналы, регистрирующие действия пользователей, исключения и события информаци-

онной безопасности, для оказания помощи в будущих расследованиях и мониторинге управления доступом.

Руководство по реализации

Контрольные журналы должны включать, где необходимо:

a) ID пользователей;
b) даты и время входа и выхода, подробности ключевых событий;
c) идентификатор терминала или его местоположение, если возможно;
d) записи успешных и отклоненных попыток доступа к системе;
e) записи успешных и отклоненных попыток доступа к данным и другим ресурсам;
f) изменения в конфигурации системы;
g) использование привилегий;
h) применение вспомогательных программ и приложений системы;
i) файлы, к которым совершён доступ, и тип доступа;
j) адреса протоколы сети;
k) системы аварийной сигнализации системы контроля доступа;
l) активация и деактивация систем защиты, таких как антивирусные системы и системы обнаружения проникновения.

Дополнительная информация

Контрольные журналы могут содержать интрузивные и конфиденциальные персональные данные. Здесь необходимо выработать соответствующие меры защиты личности. По возможности системные администраторы не должны иметь права стирать или дезактивировать записи своих собственных действий (см. 10.1.3).

10.10.2 Применение системного мониторинга

Определение

Должны быть установлены процедуры применения мониторинга средств обработки информации, а результаты действий по мониторингу должны регулярно просматриваться.

Руководство по реализации

Уровень мониторинга конкретных средств обработки информации следует определять на основе оценки рисков. Организация должна удовлетворять все юридические требования, применяемые к действиям мониторинга. При мониторинге следует обращать внимание на:

a) авторизованный доступ, включая следующие детали:
   1) пользовательский ID;
   2) даты и время основных событий;
   3) типы событий;
   4) файлы, к которым был осуществлен доступ;
   5) используемые программы/утилиты;
b) все привилегированные действия, такие как:
   1) использование привилегированных учетных записей, например, супервизора, корневого каталога, администратора;
   2) запуск и остановка системы;
   3) подсоединение/отсоединение устройства ввода/вывода;
c) попытки несанкционированного доступа, такие как:
   1) неудавшиеся или отвергнутые действия пользователя;
   2) неудавшиеся или отвергнутые действия, затрагивающие данные и другие ресурсы;
   3) нарушения политики доступа и уведомления сетевых шлюзов и межсетевых экранов;

4) предупреждения от собственных систем обнаружения вторжения;

d) предупреждения или отказы системы, такие как:
   1) консольные (терминальные) предупреждения или сообщения;
   2) исключения, записанные в системные журналы регистрации;
   3) предупредительные сигналы, связанные с управлением сетью.
   4) сигналы тревоги, создаваемые системой контроля доступа;

e) изменения или попытки изменить установки и средства управления безопасностью системы.

Как часто результаты мониторинговой деятельности пересматриваются должно зависеть от включённых рисков. Факторы риска, которые необходимо при этом учитывать, включают:

a) критичность процессов, которые поддерживаются бизнес-приложениями;
b) стоимость, важность и критичность информации;
c) предшествующие случаи проникновения в систему и неправильное использование системы, и частота использованных уязвимостей;
d) степень взаимосвязи информационных систем организациями (особенно с общедоступными сетями);
e) выключение устройства регистрации.

Дополнительная информация

Процедуры мониторинга применения необходимы для того, чтобы пользователи выполняли только явно санкционированные действия.

Просмотр журнала включает понимание угроз, стоящих перед системой и то, как они могут реализоваться. Примеры событий, которые могут потребовать дальнейшего расследования в случае появления инцидентов нарушения информационной безопасности, даны в 13.1.1.

10.10.3 Защита информации журнала

Определение

Средства регистрации и информация журнала должны быть защищены от тайных действий и несанкционированного доступа.

Руководство по реализации

Средства защиты должны быть направлены на защиту от несанкционированных изменений и эксплуатационных проблем, связанных со средствами регистрации, включая:

a) изменения в типах сообщения, которые регистрируются;
b) редактирование или стирание системных журналов;
c) превышение ёмкости носителей системных журналов, приводящее или к сбою в регистрации событий, или положению записи на ранее зарегистрированные события.

Может потребоваться архивирование некоторых контрольных журналов как часть политики сохранения записей или как требование по сбору и сохранению свидетельств (см. 13.2.3).

Дополнительная информация

Системные журналы регистрации часто содержат информацию, значительный объем которой не представляет интереса с точки зрения мониторинга безопасности. Для облегчения идентификации существенных событий при мониторинге безопасности, целесообразно рассмотреть возможность автоматического копирования соответствующих типов сообщений в отдельный журнал, и/или использовать подходящие системные утилиты или инструментальные средства аудита для подготовки данных анализа.

Системные журналы необходимо защитить, поскольку, если их данные можно модифицировать или стереть, их существование может создать ложное чувство защищённо-

сти.

10.10.4 Журналы администратора и оператора

Определение

Действия системного администратора и системного оператора должны регистрироваться.

Руководство по реализации

Журналы должны включать:

a) время возникновения события (успешного или неудачного);
b) информацию о событии (например, обработанных файлах) или отказе в работе (например, о появлении ошибки и предпринятых коррективных действиях);
c) какая учётная запись и какой администратор или оператор были задействованы;
d) какие процессы были задействованы.

Журналы оператора и администратора должны просматриваться на регулярной основе.

Дополнительная информация

Для мониторинга на соответствие действий администрации системы и сети может использоваться система обнаружения вторжения, управляемая вне области управления администраторов системы и сети.

10.10.5 Регистрация неисправностей

Определение

Дефекты должны регистрироваться, анализироваться и корректироваться.

Руководство по реализации

Необходимо регистрировать сообщения пользователей или системных программ об ошибках связанных с обработкой информации или системами связи. Должны существовать четкие правила обработки допущенных ошибок, включающие:

a) анализ ошибок для обеспечения уверенности в том, что они были удовлетворительным образом устранены;
b) анализ предпринятых корректирующих мер обеспечивающих уверенность в том, что мероприятия по управлению информационной безопасностью не были скомпрометированы (нарушены) и предпринятые действия надлежащим образом санкционированы.

Необходимо обеспечить реализацию системной функции регистрации ошибок при её наличии.

Дополнительная информация

Регистрация ошибок и дефектов может повлиять на функционирование системы. Подобная регистрация должна осуществляться квалифицированным персоналом и уровень регистрации, требуемый для отдельных систем, должен определяться оценкой риска, учитывая ухудшение качества функционирования.

10.10.6 Синхронизация часов

Определение

Часы всех соответствующих систем обработки информации внутри организации или сферы безопасности должны быть синхронизированы с помощью единого источника точного времени.

Руководство по реализации

Там, где компьютер или устройство связи имеют возможность использовать часы в реальном времени, их следует устанавливать по Универсальному Скоординированному

Времени (UCT) или стандартному местному времени. Так как некоторые часы, как известно, "уходят вперед" или "отстают", должна быть процедура, которая проверяет и исправляет любое значимое изменение.

Для того, чтобы временная метка отражала реальные дату/время, необходима правильная интерпретация формата дата/время. Необходимо принимать во внимание местную специфику (например, смена летнего времени на зимнее и наоборот).

Дополнительная информация

Правильная установка компьютерных часов (таймера) важна для обеспечения точности журналов аудита, которые могут потребоваться для расследований или как доказательство при судебных или административных разбирательствах. Некорректные журналы аудита могут затруднять такие расследования, а также вести к сомнению в достоверности собранных доказательств. В качестве главных электрочасов для регистрирующих систем могут использоваться часы, соединённые с трансляцией сигналов точного времени от национальных атомных часов. Для поддержания синхронизации всех серверов с главными электрочасами может применяться протокол времени сети.

11 Контроль доступа

11.1 Требование бизнеса по обеспечению контроля доступа

Цель: контроль доступа к информации.

Доступ к информации, средствам обработки информации и бизнес-процессам должен быть контролируемым с учетом требований бизнеса и безопасности.

Требования к контролю доступа должны быть отражены в политиках в отношении распространения и авторизации информации.

11.1.1 Политика контроля доступа

Определение

Политика контроля доступа должна устанавливаться, документироваться на основе требований бизнеса и безопасности для доступа.

Руководство по реализации

Правила контроля доступа и права каждого пользователя или группы пользователей следует четко определить политику в отношении логического доступа. Меры контроля и логического и физического доступа (см. также раздел 9) должны рассматриваться вместе. Пользователи и поставщики услуг должны быть оповещены о необходимости выполнения требований в отношении логического доступа.

Необходимо, чтобы в политике было учтено следующее:

a) требования безопасности конкретных бизнес-приложений;
b) идентификацию всей информации, связанной с функционированием бизнес-приложений и рисков информации, с которыми сталкиваются;
c) политики в отношении распространения информации и авторизации доступа, например, применение принципа "need to know" (пользователь получает доступ только к данным, безусловно необходимым ему для выполнения конкретной функции), а также в отношении классификации информации и требуемых уровней защиты (см. 7.2);
d) согласованность между политиками по контролю доступа и классификации информации применительно к различным системам и сетям;
e) применимое законодательство и любые договорные обязательства относительно защиты доступа к данным или сервисам (см. 15.1);
f) стандартные профили доступа пользователей для типовых обязанностей в ор-

ганизации;

g) управление правами доступа в распределенной сети с учетом всех типов доступных соединений.
h) разделение ролей контроля доступа, например, запрос доступа, санкционирование доступа, управление доступом
i) требования для формального санкционирования запросов доступа (см.11.2.1);
j) требования по периодическому пересмотру средств контроля доступа (см.11.2.4);
k) аннулирование прав доступа (см. 8.3.3).

Дополнительная информация

Следует принимать во внимание, при определении правил контроля доступа следующее:

a) дифференциацию между правилами, обязательными для исполнения и правилами руководствами, которые являются общими или применяемыми при определенных условиях;
b) установление правил, основанных на предпосылке "все должно быть в общем случае запрещено, пока явно не разрешено", а не на более слабом принципе "все в общем случае разрешено, пока явно не запрещено";
c) изменения в признаках маркировки информации (см. 7.2), как генерируемых автоматически средствами обработки информации, так и инициируемых по усмотрению пользователей;
d) изменения в правах пользователя, как устанавливаемых автоматически информационной системой, так и определенных администратором;
e) правила, которые требуют одобрения другого лица перед применением, а также тех, которые не требуют специального одобрения

Правила контроля доступа должны поддерживаться формальными процедурами и чётко определёнными обязательствами (см., например, 6.1.3, 11.3, 10.4.1, 11.6).

11.2 Управление доступом пользователя

Цель: Обеспечение санкционированного доступа пользователя и предотвращение несанкционированного доступа к информационным системам.

Должны быть в наличии формальные процедуры контроля за распределением прав доступа к информационным системам и службам.

Процедуры должны охватывать все стадии жизненного цикла доступа пользователя от начальной регистрации новых пользователей до конечной отмены регистрации пользователей, которым больше не нужен доступ к информационным системам к службам. Особое внимание нужно уделить необходимости контролировать распределение привилегированных прав доступа, которые позволяют пользователям обходить средства контроля системы.

11.2.1 Регистрация пользователей

Определение

В наличии должна быть формальная процедура регистрации и отмены регистрации пользователей для предоставления и аннулирования доступа ко всем информационным системам и службам.

Руководство по реализации

Процедура контроля доступа по отношению к регистрации и отмены регистрации пользователей должна включать:

a) использование уникальных ID (идентификаторов, или имен) пользователей та-

ким образом, чтобы действия в системе можно было бы соотнести с пользователями и установить ответственных. Использование групповых ID следует разрешать только в тех случаях, где это необходимо по бизнес или операционных причин, и это должно приниматься и документироваться;

b) проверку того, что пользователь имеет авторизацию от владельца системы на пользование информационной системой или сервисов. Кроме того, может быть целесообразным наличие дополнительного разрешения на предоставление прав от руководства;

c) проверку того, что уровень предоставленного доступа соответствует производственной необходимости (11.1), а также учитывает требования политики безопасности организации, например, не нарушает принципа разделения обязанностей (10.1.3);

d) предоставление пользователям письменного документа, в котором указаны их права доступа;

e) требование того, чтобы пользователи подписывали документ о том, что они понимают условия предоставления доступа;

f) обеспечение уверенности в том, что поставщики услуг не предоставляют доступ, пока процедуры авторизации не завершены;

g) ведение формализованного учета в отношении всех лиц, зарегистрированных для использования сервисов;

h) немедленную отмену или блокирование прав доступа пользователей, у которых изменились должностные обязанности или уволившихся из организации;

i) периодическую проверку и удаление или блокирование избыточных пользовательских ID и учетных записей (см. 11.2.4);

j) обеспечение того, чтобы избыточные пользовательские ID не были переданы другим пользователям.

Дополнительная информация

Необходимо уделить внимание определению ролей доступа пользователей, основанных на бизнес-требованиях, которые суммируют права доступа в типичные профили доступа пользователей. Запросами и просмотрами доступа (см. 11.2.4) управлять легче на уровне таких ролей, чем на уровне определённых прав.

Необходимо рассматривать возможность включения положений о применении соответствующих санкций в случае попыток неавторизованного доступа в трудовые договора сотрудников и контракты с поставщиками услуг (6.1.5, 8.1.3 и 8.2.3).

11.2.2 Менеджмент привилегий

Определение

Предоставление и использование привилегий необходимо ограничивать и держать под контролем.

Руководство по реализации

Необходимо, чтобы в многопользовательских системах, которые требуют защиты от неавторизованного доступа, предоставление привилегий контролировалось посредством формализованного процесса авторизации. Необходимо рассматривать принятие следующих мер:

a) необходимо идентифицировать привилегии доступа в отношении каждого системного продукта, например, операционной системы, системы управления базами данных и каждого бизнес-приложения, а также пользователи, которым эти привилегии должны быть предоставлены;

b) привилегии должны предоставляться только тем сотрудникам, которым это не-

обходимо для работы и только на время каждого такого случая необходимости в соответствии с политикой контроля доступа (11.1.1), например, предоставляя минимальные возможности по работе с системой для выполнения требуемых функций, только когда в этом возникает потребность;

c) необходимо обеспечивать процесс авторизации и регистрацию всех предоставленных привилегий. Привилегии не должны предоставляться до завершения процесса авторизации;

d) следует проводить политику разработки и использования стандартных системных утилит (скриптов) для того, чтобы избежать необходимости в предоставлении дополнительных привилегий пользователям;

e) следует проводить разработки и исследования программ, чтобы избежать необходимости связываться с привилегиями;

f) следует использовать различные идентификаторы пользователей при работе в обычном режиме и с использованием привилегий.

Дополнительная информация

Неадекватное использование привилегий (любая особенность или средство информационной системы, которое позволяет пользователю подменить меры контроля системы или приложения) может быть главной причиной сбоев или образования брешей в системах.

11.2.3 Контроль в отношении паролей пользователей

Определение

Предоставление паролей должно контролироваться посредством формализованного процесса управления.

Руководство по реализации

Процесс должен включать следующие требования:

a) подписание пользователями документа о необходимости соблюдения полной конфиденциальности личных паролей, а в отношении групповых паролей - соблюдения конфиденциальности в пределах рабочей группы, это может быть включено в условия трудового договора (см. 8.1.3);

b) в случаях, когда от пользователей требуется управление собственными паролями, необходимо обеспечить предоставление безопасного первоначального временного пароля, который пользователи принуждаются сменить при первой регистрации в системе;

c) определение процедур проверки идентичности пользователя до предоставления ему нового пароля, пароля замены или временного пароля;

d) обеспечение безопасного способа выдачи временных паролей пользователям. Следует избегать использования незащищенных (открытый текст) сообщений электронной почты или сообщений по электронной почте от третьей стороны;

e) временные пароли должны быть уникальными для получающего их лица и не должны быть легко угадываемыми;

f) пользователям необходимо подтверждать получение паролей;

g) пароли никогда не следует хранить в компьютерной системе в незащищенной форме;

h) после установки систем или программного обеспечения пароли по умолчанию продавца должны быть изменены.

Дополнительная информация

Пароли являются наиболее распространенными средствами подтверждения идентификатора пользователя при доступе к информационной системе или сервису согласно авторизации пользователей. При необходимости, следует рассматривать возможности дру-

гих технологий для идентификации и аутентификации пользователя, такие как биометрия (проверка отпечатков пальцев), проверка подписи, и использование аппаратных средств идентификации (смарт - карт).

11.2.4 Пересмотр прав доступа пользователей

Определение

Руководство должно регулярно пересматривать права доступа пользователей, используя формальный процесс.

Руководство по реализации

При пересмотре прав доступа необходимо рассмотреть следующие правила:

a) права доступа пользователей должны пересматриваться регулярно, рекомендуемый период 6 месяцев, и после любых изменений, таких как: продвижение, понижение, окончание договора о трудоустройстве (см. 11.2.1);
b) при переводе пользователя из одного подразделения в другое внутри организации его права должны пересматриваться и перераспределяться;
c) авторизации специальных привилегированных прав доступа (11.2.2) должны осуществляться через меньшие интервалы времени (например, период 3 месяца);
d) предоставленные привилегии должны периодически проверяться для обеспечения уверенности в том, что не были получены неавторизованные привилегии;
e) изменения в привилегированных учётных записях должны регистрироваться для периодического пересмотра.

Дополнительная информация

Для поддержания эффективного контроля за доступом к данным и информационным службам права доступа пользователей должны регулярно пересматриваться.

11.3 Обязанности пользователя

Цель: предотвращение неавторизованного доступа пользователей к информации, и компрометации или кражи информации и средств обработки информации.

Взаимодействие авторизованных пользователей является важным аспектом эффективной безопасности.

Необходимо, чтобы пользователи были осведомлены о своих обязанностях по использованию эффективных мероприятий по управлению информационной безопасностью доступа, в частности, в отношении паролей и безопасности оборудования, с которым они работают.

Для снижения риска несанкционированного доступа или нанесения ущерба документам, носителям информации и средствам обработки информации необходимо реализовать политику «чистого стола» и «чистого экрана».

11.3.1 Использование пароля

Определение

От пользователей требовать соблюдения правил безопасности при выборе и использовании паролей.

Руководство по реализации

Все пользователи должны быть осведомлены о необходимости:

a) сохранения конфиденциальности паролей;
b) избегать делать записи (например, на бумаге, в файлах программного обеспечения или портативном устройстве) паролей, без гарантии их безопасного хра-

нения и утверждения метода хранения;

c) изменения паролей всякий раз, при наличии любого признака возможной компрометации системы или пароля;

d) выборе качественных паролей с минимальной длиной, которые:

1) легко запомнить;

2) не подвержены легкому угадыванию или вычислению с использованием персональной информации, связанной с владельцем пароля, например, имен, номеров телефонов, дат рождения и т.д.;

3) неуязвимы для словарных атак (т.е. не состоят из слов, включённых в словари);

4) не содержат последовательных идентичных символов, и не состоят из полностью числовых или полностью буквенных групп;

e) изменении паролей через равные интервалы времени или после определенного числа доступов и исключении повторного или цикличного использования старых паролей (пароли для привилегированных учетных записей следует менять чаще, чем обычные пароли);

f) изменении временных паролей при первой регистрации в системе;

g) запрещении включения паролей в автоматизированный процесс регистрации, например, с использованием хранимых макрокоманд или функциональных клавиш;

h) исключении коллективного использования индивидуальных паролей;

i) не использовать один и тот же пароль для деловых и неделовых целей.

Если пользователи нуждаются в доступе к многочисленным услугам, системам или бизнес-приложениям, и вынуждены использовать многочисленные пароли, можно порекомендовать возможность использования одного качественного пароля (см.d)) для всех сервисов, обеспечивающих разумный уровень защиты хранимого пароля в каждой услуге, системе или бизнес-приложении.

Дополнительная информация

Управление системой «справочного стола», имеющей дело с утерянными или забытыми паролями, требует особой осторожности, поскольку это может стать средством атаки на систему паролей.

11.3.2 Оборудование, оставленное пользователем без присмотра

Определение

Пользователи должны обеспечивать соответствующую защиту оборудования, оставленного без присмотра.

Руководство по реализации

Всем пользователям необходимо знать требования безопасности и методы защиты оставленного без присмотра оборудования, также как и свои обязанности по обеспечению такой защиты. Пользователям рекомендуется:

a) завершать активные сеансы по окончании работы, если отсутствует механизм блокировки, например, хранитель экрана, защищенный паролем;

b) отключаться от мэйнфрейма, серверов и офисных компьютеров, когда сеанс закончен (то есть не только выключать экран PC или терминал);

c) защищать PC или терминалы от неавторизованного использования посредством замка или эквивалентного средства контроля, например, защита доступа с помощью пароля, когда оборудование не используется (см. также 11.3.3).

Дополнительная информация

Для оборудования, установленного на рабочих местах пользователя, например, рабочей станции или файловых серверах, может потребоваться особая защита от несанкционированного доступа, когда это оборудование остаётся без присмотра длительное время.

11.3.3 Политика «чистого стола» и «чистого экрана»

Определение

Необходимо принять чёткую политику «чистого стола» для служебных документов и съёмных носителей информации и политику «чистого экрана» для оборудования по обработке информации.

Руководство по реализации

При применении политик «чистого стола» и «чистого экрана» следует учитывать классификацию информации с точки зрения безопасности (см. 7.2), юридические и контрактные требования (см. 15.1) и соответствующие риски, а также корпоративную культуру организации. Следует применять следующие мероприятия по управлению информационной безопасностью:

a) носители с важной или критичной служебной информацией, например, на бумажном или электронном носителе, когда она не требуется, следует убирать и запирать (идеально, в несгораемом сейфе или шкафу), особенно когда помещение пустует;
b) компьютеры и терминалы должны оставляться выключенными из сети или защищёнными экраном и механизмом блокировки клавиатуры, контролируемыми паролем, жетоном или подобным им механизмом идентификации пользователя, когда остаются без присмотра, и должны быть защищены блокировкой клавиши, паролями и другими средствами контроля, когда не используются долгое время;
c) необходимо обеспечить защиту пунктов отправки/приема корреспонденции, а также факсимильных и телексных аппаратов в случаях нахождения последних без присмотра;
d) фотокопировальное и другое множительное оборудование (например, сканеры, цифровые камеры) должны быть защищены от несанкционированного доступа;
e) документы с секретной или конфиденциальной информацией должны немедленно удаляться из принтеров.

Дополнительная информация

Политика «чистого стола/чистого экрана» снижает риски несанкционированного доступа, утерю или нанесения ущерба информации в рабочее или нерабочее время. Для защиты от таких бедствий, как пожар, землетрясение, наводнение или взрыв могут также использоваться сейфы и другие средства безопасного хранения.

Рассмотрите возможность использования принтеров с функцией пин-кода, когда только авторы могут получить свои распечатки и то, только стоя рядом с принтером.

11.4 Контроль сетевого доступа

Цель: Предотвращение несанкционированного доступа к сетевым сервисам.

Доступ, как к внутренним, так и к внешним сетевым сервисам, должен быть контролируемым.

Доступ пользователя к сетям и сетевым сервисам не должен создавать угрозы безопасности сетевых сервисов, обеспечивая:

a) соответствующие интерфейсы между сетью организации и сетями, принадлежащими другим организациям, или общедоступными сетями;
b) соответствующие механизмы аутентификации в отношении пользователей и оборудования;
c) задействование контроля доступа пользователей к информационным сервисам.

11.4.1 Политика в отношении использования сетевых служб

Определение

Пользователям следует обеспечивать непосредственный доступ только к тем сервисам, в которых они были авторизованы.

Руководство по реализации

Следует предусматривать меры безопасности в отношении использования сетей и сетевых сервисов. При этом должны быть определены:

a) сети и сетевые услуги, к которым разрешен доступ;
b) процедуры авторизации для определения того, кому, к каким сетям и сетевым сервисам разрешен доступ;
c) мероприятия и процедуры по защите от несанкционированного подключениям к сетевым сервисам;
d) средства, использующиеся для доступа к сетям и сетевым службам (например, условия для наборного доступа к Интернет или удалённой системе).

Необходимо, чтобы эти меры согласовывались с требованиями бизнеса в отношении контроля доступа (11.1).

Дополнительная информация

Несанкционированные и небезопасные соединения к сетевым службам могут повлиять на всю организацию. Контроль доступа, в частности, является важным для сетевых подключений к важным или критичным бизнес-приложениям или для пользователей, находящихся в зонах высокого риска, например, в общественных местах или за пределами организации, то есть вне сферы непосредственного управления и контроля безопасности со стороны организации.

11.4.2 Аутентификация пользователей в случае внешних соединений

Определение

Для контроля доступа удалённых пользователей должны использоваться соответствующие методы аутентификации.

Руководство по реализации

Аутентификация удаленных пользователей может быть достигнута при использовании средств криптографии, аппаратных средств защиты (маркеров, токенов) или протоколов, поддерживающих метод "отклик-отзыв". Возможные реализации подобных методов могут быть найдены в различных решениях виртуальной частной сети (VPN). Выделенные частные линии могут также использоваться для обеспечения доверия к источнику подключений.

Процедуры и средства контроля обратного вызова, например, использование модемов с обратным вызовом, могут обеспечивать защиту от неавторизованных и нежелательных подключений к средствам обработки информации организации, так как подтверждают право на доступ пользователей, пытающихся установить удаленную связь с сетью организации. При использовании этих способов, организации не следует использовать сетевые сервисы, которые включают переадресацию вызова. Если же они используются, необходимо блокировать возможности переадресации, чтобы избежать связанных с этим рисков. Процесс обратного вызова должен обеспечивать уверенность в том, что фактическое разъединение на стороне организации осуществлено. В противном случае, удаленный пользователь мог бы держать линию занятой, фальсифицируя проверку обратного вызова. Для исключения подобных инцидентов процедуры и средства контроля обратного вызова следует тщательно тестировать.

Аутентификация узла может служить альтернативным средством аутентифицирования групп удаленных пользователей там, где они подсоединены к безопасному компьютерному средству совместного использования. Для аутентификации узлов могут исполь-

зоваться криптографические методы, например, основанные на машинных сертификатах. Это является частью нескольких решений, основанных на применении виртуальных частных сетей.

Для контроля доступа к беспроводным сетям могут применяться дополнительные средства контроля аутентификации. Особую осторожность необходимо соблюдать при, выборе средств защиты беспроводных сетей вследствие больших возможностей необнаруженного перехвата и внедрения сетевого трафика.

Дополнительная информация

Внешние соединения обеспечивают потенциал для неавторизованного доступа к служебной информации, например, при использовании телефонной связи. Некоторые методы аутентификации обеспечивают больший уровень защиты, чем другие, например, методы, основанные на использовании средств криптографии и могут обеспечить надежную аутентификацию. Исходя из оценки риска, важно определить требуемый уровень защиты для выбора соответствующего метода аутентификации.

Средство автоматического подсоединения к удаленному компьютеру может предоставить способ получения неавторизованного доступа к бизнес-приложению. Это особенно важно, если подключение производится к сети, которая находится вне сферы контроля управления безопасностью организации.

11.4.3 Идентификация оборудования в сетях

Определение

Автоматическая идентификация оборудования должна рассматриваться как средство для различения типов оборудования и места его расположения.

Руководство по реализации

Идентификация оборудования может применяться, если имеет значение инициирование связи из специфического местоположения или оборудования. Для указания, разрешено ли этому оборудованию подсоединение к сети, может использоваться идентификатор, встроенный в оборудование или приданный ему. Эти идентификаторы должны показывать, к какой сети разрешено подсоединять оборудование, если имеются несколько сетей и, в особенности, если эти сети имеют разную степень секретности. Может возникнуть необходимость рассмотреть физическую защиту оборудования для поддержания безопасности его идентификатора.

Дополнительная информация

Этот контроль можно осуществить другими методами для аутентификации пользователя оборудования (см. 11.4.2). Идентификация оборудования может быть дополнена аутентификацией пользователя.

11.4.4 Защита дистанционных портов диагностики и конфигурации

Определение

Физический и логический доступ к портам диагностики и конфигурации должен быть под контролем.

Руководство по реализации

Потенциальные средства контроля доступа к портам диагностики и конфигурации включают использование блокировки клавиши и вспомогательные процедуры контроля физического доступа к порту. Примером такой процедуры является предоставление доступа к портам диагностики и конфигурации при условии договорённости между руководителем вычислительной службы и вспомогательным персоналом, занимающимся программным обеспечением и аппаратными средствами и нуждающемуся в доступе.

Порты, сервисы и подобные им устройства, установленные на компьютерном или сетевом оборудовании, которые необязательны для обеспечения деловой деятельности,

должны быть отключены от сети или удалены.

Дополнительная информация

Многие компьютерные, сетевые системы и системы связи устанавливаются вместе со средствами диагностики и конфигурации, которые используются инженерами по обслуживанию. При отсутствии защиты эти диагностические порты могут стать средством несанкционированного доступа.

11.4.5 Разделение в сетях

Определение

В сетях группы информационных служб, пользователей и информационных систем должны быть разделены.

Руководство по реализации

Одно из таких мероприятий состоит в том, чтобы разделять их на отдельные логические сетевые домены, например, внутренний сетевой домен организации и внешние сетевые домены, каждый из которых защищен определенным периметром безопасности. Градуированные наборы мер контроля могут применяться в различных доменах логической сети для дальнейшего разделения сред безопасности сети, например, общедоступные системы, внутренние сети и критические активы. Домены должны определяться, основываясь на оценке риска и различных требованиях в каждом из доменов. Такой сетевой периметр может быть реализован посредством внедрения шлюза безопасности между двумя связанными сетями для контроля доступа и информационного потока между ними. Этот шлюз следует конфигурировать для фильтрации трафика между доменами (11.4.6 и 11.4.7) и для блокирования неавторизованного доступа в соответствии с политикой контроля доступа организации (11.1). Примером такого шлюза является межсетевой экран. Другой метод разделения логических доменов – это ограничить сетевой доступ, используя виртуальные частные сети для групп пользователей внутри организации.

Сети можно также разделить с помощью функциональных возможностей сетевых устройств, например, IP-переключения. Затем отдельные домены можно реализовать путём контролирования потоков сетевых данных, используя возможности маршрутизации/переключения, таких как списки контроля доступа.

Критерии для разделения сетей на домены следует основывать на политике контроля доступа (10.1), а также учитывая последствия этого разделения для производительности в результате включения подходящей технологии маршрутизации сетей или шлюзов (11.4.6 и 11.4.7).

Кроме того, разделение сетей должно основываться на ценности и засекреченности информации, хранящихся или обрабатываемых в сетях, уровнях доверия или сферах деятельности для уменьшения общего воздействия.

Необходимо рассмотреть проблему отделения беспроводных сетей от внутренних или частных сетей. Поскольку периметры беспроводных сетей определены нечётко, для идентификации средств контроля необходимо провести оценку рисков (например, строгая аутентификация, криптографические методы и частотная селекция) в целях поддержания сетевого разделения.

Дополнительная информация

Компьютерные сети все более распространяются за пределы организации, поскольку создаются деловые партнерства, которые требуют тесного общения между партнерами или совместного использования сетевой инфраструктуры и средств обработки информации. Такие расширения увеличивают риск неавторизованного доступа к информационным системам сети, причем в отношении некоторых из этих систем, вследствие их важности или критичности, может потребоваться защита от пользователей, получивших доступ к другим системам сети.

11.4.6 Контроль сетевых соединений

Определение

По отношению к совместно используемым сетям, особенно тем, которые выходят за пределы организации, возможность пользователей подсоединяться к сети должна быть ограничена соответственно политике контроля доступа и требованиям по бизнес-приложениям (см. 11.1).

Руководство по реализации

Права доступа пользователей к сети должны поддерживаться и корректироваться соответственно политике контроля доступа (см. 11.1.1).

Возможности пользователей к соединению могут быть ограничены использованием межсетевых интерфейсов, которые фильтруют трафик при помощи заранее определённых таблиц или правил. Примерами применений, к которым должны быть применены ограничения, являются:

a) передача сообщений, например, электронная почта;
b) передача файлов;
c) интерактивные доступ;
d) доступ к приложениям.

Необходимо рассмотреть права на доступ к сети к определённому времени или дате.

Дополнительная информация

Для совместно используемых сетей, особенно тех, которые выходят за границы организации для соответствия политике контроля доступа может потребоваться объединение средств контроля в целях ограничения возможностей пользователей к подсоединению.

11.4.7 Контроль за маршрутизацией сетей

Определение

Для того чтобы компьютерные соединения и информационные потоки не нарушали политику контроля доступа к бизнес-приложениям, для сетей необходимо реализовать средства контроля за маршрутизацией.

Руководство по реализации

Средства контроля за маршрутизацией должны быть основаны на механизмах проверки позитивных адресов источника (информации) и назначения.

Для проверки адресов источника и назначения во внутренних и внешних контрольных точках сети можно использовать безопасные интерфейсы, если задействуются модуль доступа и/или технологии трансляции сетевого адреса. Конструкторы должны знать преимущества и недостатки любых применяемых механизмов. Требования по контролю за маршрутизацией сетей должны основываться на политике контроля доступа (см. 11.1).

Дополнительная информация

Для совместно используемых сетей, особенно тех, которые выходят за пределы организации, могут потребоваться дополнительные средства контроля за маршрутизацией. Это особенно относится к случаям, когда сети используются совместно с пользователями третьей стороны.

11.5 Контроль доступа к операционной системе

Цель: Предотвращение несанкционированного доступа к операционной системе

Следует использовать средства информационной безопасности для ограничения доступа несанкционированных пользователей к действующим системам. Эти средства должны обеспечивать:

a) аутентификацию санкционированных пользователей в соответствии с определённой политикой контроля доступа;
b) регистрацию успешных и неудавшихся доступов к системе;
c) регистрацию использования специальных системных привилегий;
d) выдачу сигналов тревоги при нарушении политик безопасности системы;
e) предоставление подходящих средств аутентификации;
f) ограничение времени подсоединения пользователей, в случае необходимости.

11.5.1 Процедуры безопасного входа в систему

Определение

Доступ в операционную систему должен контролироваться процедурой безопасного входа в систему.

Руководство по реализации

Процедуру регистрации в компьютерной системе следует проектировать так, чтобы свести к минимуму возможность неавторизованного доступа и не оказывать ненужной помощи неавторизованному пользователю. Правильно спланированная процедура регистрации должна обладать следующими свойствами:

a) не отображать наименований системы или приложений, пока процесс регистрации не будет успешно завершен;
b) отображать общее уведомление, предупреждающее, что доступ к компьютеру могут получить только авторизованные пользователи;
c) не предоставлять сообщений-подсказок в течение процедуры регистрации, которые могли бы помочь неавторизованному пользователю;
d) подтверждать информацию регистрации только по завершении ввода всех входных данных. В случае ошибочного ввода, система не показывает, какая часть данных является правильной или неправильной;
e) ограничивать число разрешенных неудачных попыток регистрации, например три, и предусматривать:
   1) запись неудачных и удачных попыток;
   2) включение временной задержки прежде, чем будут разрешены дальнейшие попытки регистрации, или отклонение любых дальнейших попыток без специальной авторизации;
   3) разъединение сеанса связи передачи данных;
   4) посылку тревожного сообщения на системный пульт, если число попыток входа в систему достигло максимума;
   5) установку некоторого числа повторных попыток использования пароля вместе с минимальной длиной пароля и ценностью защищаемой системы;
f) ограничивать максимальное и минимальное время, разрешенное для процедуры регистрации. Если оно превышено, система должна прекратить регистрацию;
g) фиксировать информацию в отношении успешно завершенной регистрации:
   1) дату и время предыдущей успешной регистрации;
   2) детали любых неудачных попыток регистрации, начиная с последней успешной регистрации;
h) не отображать вводимый пароль или рассмотреть возможность сокрытия знаков пароля символами;
i) не передавать пароли по сети открытым текстом.

Дополнительная информация

Если пароли передаются по сети открытым текстом во время сеанса «входа в систе-

му», они могут быть перехвачены программой сетевого анализатора пакетов.

11.5.2 Идентификация и аутентификация пользователя

Определение

Необходимо, чтобы все пользователи имели уникальный идентификатор (пользовательский ID) для их единоличного использования и должен быть выбран подходящий метод аутентификации, чтобы доказать требуемую идентичность пользователя.

Руководство по реализации

Этот метод должен применяться ко всем типам пользователей (включая персонал технической поддержки, т. е. операторов, администраторов сети, системных программистов и администраторов базы данных).

Пользовательские ID должны использоваться, чтобы проанализироваться ответственным лицом. Регулярные действия пользователей не должны выполняться от привилегированных учётных записей.

Для выполнения особо важных работ допустимо использовать общий идентификатор для группы пользователей или для выполнения определенной работы. В таких случаях необходимо соответствующим образом оформленное разрешение руководства. Кроме того, для обеспечения безопасности системы от неавторизованного доступа в этих случаях может потребоваться применение дополнительных мер обеспечения информационной безопасности.

Применение общих идентификаторов одним лицом может быть разрешено только в случаях, когда нет необходимости прослеживать доступные функции иди действия, выполненные идентификатором (например, доступ только для чтения, или где есть в наличии другие средства контроля (например, пароль для общего идентификатора выдаётся только одному штату служащих за раз, и такой случай регистрируется).

Там, где требуется строгая проверка аутентификации и идентификации, должны использоваться методы аутентификации, альтернативные паролям, такие как шифровальные средства, смарт-карты, жетоны или биометрические средства.

Дополнительная информация

Пароли (см. также 11.3.1 и 11.5.3) -очень распространенный способ обеспечения идентификации и аутентификации, основанный на использовании пароля, который знает только пользователь. То же самое может быть достигнуто средствами криптографии и аутентификационными протоколами. Строгость идентификации и аутентификации пользователя должна соответствовать степени секретности информации, к которой совершается доступ.

Специальные физические устройства доступа с памятью (token) или микропроцессорные карты (смарт-карты), которыми наделены пользователи, могут также использоваться для идентификации и аутентификации. Биометрические аутентификационные методы, которые основаны на уникальности характеристик (особенностей) индивидуума, могут также использоваться для аутентификации пользователя. Сочетание различных технологий и методов обеспечивает более надежную аутентификацию.

11.5.3 Система управления паролями

Определение

Системы управления паролями должны быть интерактивными и обеспечивать пароли качества

Руководство по реализации

Система управления паролированием должна:

а) предписывать использование индивидуальных паролей и пользовательских ID, для обеспечения установления ответственности;

b) позволять пользователям выбирать и изменять их собственные пароли, а также включать подтверждающую процедуру для учета ошибок ввода;
c) предписывать выбор высококачественных паролей, в соответствии с 11.3.1;
d) принуждать их к изменению паролей (см. 11.3.1);
e) вынуждать пользователей изменять временные пароли при первой регистрации (11.2.3);
f) поддерживать хранение истории предыдущих пользовательских паролей, и предотвращать их повторное использование;
g) не отображать пароли на экране при их вводе;
h) хранить файлы паролей отдельно от данных прикладных систем;
i) хранить и передавать пароли в защищённой форме (например, зашифрованной или хэшированной).

Дополнительная информация

Пароли - одно из главных средств подтверждения полномочия пользователя, осуществляющего доступ к компьютерным сервисам.

Для некоторых бизнес-приложений требуется назначение пользовательских паролей независимым должностным лицом, в таких случаях пункты перечислений 2, 4 и 5, приведенных выше, не применяются. В большинстве же случаев пароли выбираются и поддерживаются пользователями. См. 11.3.1 для руководства по использованию паролей.

11.5.4 Использование системных утилит

Определение

Использование утилит, которые способны обходить средства контроля системы и приложений, должно быть ограничено и строго контролироваться.

Руководство по реализации

Необходимо рассмотреть следующие правила использования системных утилит:

a) использование процедур идентификации, аутентификации и авторизации системных утилит;
b) отделение системных утилит от прикладных программ;
c) ограничение использования системных утилит минимальным числом доверенных авторизованных пользователей, которым это необходимо (см. также 11.2.2);
d) авторизация эпизодического использования системных утилит;
e) ограничение доступности системных утилит (только на время внесения авторизованных изменений);
f) регистрация использования всех системных утилит;
g) определение и документирование уровней авторизации в отношении системных утилит;
h) удаление или блокировка всех ненужных утилит и системного программного обеспечения;
i) непредоставление системных утилит пользователям, которые имеют доступ к приложениям в системах, в которых требуется разделение обязанностей.

Дополнительная информация

На большинстве компьютеров устанавливается, по крайней мере, одна программа - системная утилита, которая позволяет обойти меры предотвращения неавторизованного доступа к операционным системам и бизнес-приложениям.

11.5.5 Периоды бездействия сеансов

Определение

Бездействующие сеансы должны отключаться после определённого периода бездей-

ствия.

Руководство по реализации

Механизм блокировки по времени должен обеспечивать очистку экрана сеанса, а также закрытие сеансов работы приложения и сетевого сеанса после определенного периода времени бездействия. Время срабатывания блокировки должно устанавливаться с учетом рисков безопасности, классификации обрабатываемой информации и использующихся приложений, и рисков относительно пользователей оборудования.

Следует иметь ввиду, что некоторые персональные компьютеры обеспечивают ограниченную возможность блокировки терминала по времени путем очистки экрана и предотвращения неавторизованного доступа, при этом не осуществляя закрытия сеанса приложений или сетевого сеанса.

Дополнительная информация

Этот контроль имеет особое значение в местах повышенного риска, которые включают зоны общественного пользования за пределами сферы управления безопасностью организации. Сеансы должны быть выключены для предотвращения доступа несанкционированных лиц.

11.5.6 Ограничение времени соединения

Определение

Ограничения времени соединения должны обеспечивать дополнительную безопасность для приложений высокого риска.

Руководство по реализации

Эти меры по времени соединения необходимо применять для наиболее важных компьютерных приложений, особенно тех, которые связаны с терминалами, установленными в местах повышенного риска, например, в общедоступных местах или вне сферы контроля управления безопасностью организации. Примеры таких ограничений:

a) использование заранее определенных отрезков времени для пакетной передачи файлов или регулярных интерактивных сеансов небольшой продолжительности;
b) ограничение времени подключений обычными часами работы организации, если нет необходимости сверхурочной или более продолжительной работы;
c) рассмотрение необходимости повторной аутентификации через синхронизированные интервалы времени.

Дополнительная информация

Ограничение периода времени, в течение которого разрешены подсоединения к компьютерным сервисам, уменьшает интервал времени, в течение которого возможен несанкционированный доступ. Ограничение длительности активных сеансов предохраняет пользователей от блокировки сеансов, открытых, чтобы предотвратить повторную аутентификацию.

11.6 Контроль доступа к приложениям и информации

Цель: предотвращение несанкционированного доступа к данным информационных систем.

Необходимо применять меры обеспечения информационной безопасности для ограничения доступа к прикладным системам.

Логический доступ к программному обеспечению прикладных программ и информации должен быть ограничен только санкционированными пользователями. Для этого необходимо обеспечить:

a) контроль доступа пользователей к информации и функциям бизнес-

приложений в соответствии с определенной бизнесом политикой контроля доступа;

b) защиту от несанкционированного доступа любой утилиты и системного программного обеспечения и вредоносного программного обеспечения, которые позволяют обходить средства операционной системы или приложений;

c) исключение компрометации других систем, с которыми совместно используются информационные ресурсы.

11.6.1 Ограничение доступа к информации

Определение

Доступ пользователей и вспомогательного персонала к информации и функциям прикладной системы следует ограничить в соответствии с определённой политикой контроля доступа.

Руководство по реализации

Ограничения доступа должны основываться на отдельных требованиях к приложениям. Политика контроля доступа должна соответствовать политике доступа организации (см. 11.1).

Необходимо рассматривать применение следующих мероприятий по управлению информационной безопасностью для обеспечения требований по ограничению доступа:

a) поддержка меню для управления доступом к прикладным функциям системы;

b) контроль прав доступа пользователей, например, чтение/запись/удаление/ выполнение;

c) контроль прав доступа к другим приложениям;

d) обеспечение уверенности в том, что выводимые данные из бизнес-приложений, обрабатывающих важную информацию, содержали только требуемую информацию, и пересылались только в адреса авторизованных терминалов и мест назначения. Следует проводить периодический анализ процесса вывода для проверки удаления избыточной информации.

11.6.2 Изоляция систем, обрабатывающих важную информацию

Определение

Системы, обрабатывающие важную информацию, должны иметь выделенную (изолированную) вычислительную среду.

Руководство по реализации

Для изоляции систем, обрабатывающих важную информацию, следует рассмотреть следующие пункты:

a) владельцу бизнес-приложений необходимо определить и документально оформить степень их важности (7.1.2);

b) когда важное бизнес-приложение должно работать в среде совместного использования, необходимо выявить другие приложения, с которыми будет осуществляться совместное использование ресурсов, и согласовать это с владельцем важного бизнес-приложения и соответствующие риски должны идентифицироваться.

Дополнительная информация

Некоторые прикладные системы имеют очень большое значение с точки зрения безопасности данных и поэтому требуют специальных условий эксплуатации. Важность обрабатываемой информации может указывать, что прикладная система:

a) должны работать на выделенном компьютере;

b) должна осуществлять совместное использование ресурсов только с безопасными бизнес-приложениями.

Изоляция может достигаться, используя физические или логические методы (см. также 11.4.5).

11.7 Мобильные вычислительные устройства и удалённый доступ

Цель: гарантия информационной безопасности при использовании мобильных вычислительных устройств и возможности удалённого доступа.

Требуемая защита должна быть достигнута с учётом рисков, возникающих по причине особенностей работы в данных условиях. При использовании мобильных вычислительных устройств риск работы в незащищённом окружении должен быть принят во внимание и должна быть применена соответствующая защита. В случае удалённого доступа организация должна применять защиту точек удалённого доступа и гарантировать, что соответствующие мероприятия применены на месте откуда осуществляется доступ.

11.7.1 Работа с переносными вычислительными устройствами и средствами связи

Определение

Необходимо иметь в наличии формальную политику, и для защиты от рисков при использовании переносных вычислительных устройств и средств связи должны быть приняты соответствующие меры безопасности.

Руководство по реализации

При использовании переносных устройств и средств коммуникации, например, ноутбуков, карманных компьютеров, переносных компьютеров, смарт-карт и мобильных телефонов, необходимо принимать специальные меры противодействия компрометации служебной информации. Необходимо принять формализованную политику, учитывающую риски, связанные с работой с переносными устройствами, в особенности, в незащищенной среде.

Политика переносных вычислительных устройств должна включать требования по физической защите, контролю доступа, использованию средств криптографии, резервированию и защите от вирусов. Необходимо, чтобы эта политика включала также правила и рекомендации по подсоединению мобильных средств к сетям, а также руководства по использованию этих средств в общедоступных местах.

Следует проявлять осторожность при использовании мобильных средств вычислительной техники и других сервисных средств в общедоступных местах, переговорных комнатах и других незащищенных помещениях вне организации. Чтобы избегать неавторизованного доступа или раскрытия информации, хранимой и обрабатываемой этими средствами необходимо обеспечить защиту с использованием средств криптографии (12.3).

Пользователи мобильных средств связи в общественных местах должны быть осторожны, чтобы уменьшить риск "подсмотра" паролей доступа неавторизованными лицами. Необходимо внедрять и поддерживать в актуализированном состоянии средства и способы защиты от вредоносного программного обеспечения (10.4).

Следует регулярно осуществлять резервирование критической бизнес-информации. Следует также обеспечить доступность оборудования для быстрого и удобного резервирования информации. Необходимо обеспечить адекватную защиту резервных копий от кражи или потери информации.

Соответствующую защиту необходимо обеспечить мобильным средствам, подсоединенным к общедоступным сетям. Удаленный доступ к служебной информации через общедоступную сеть с использованием мобильных средств вычислительной техники следует осуществлять только после успешной идентификации и аутентификации, а также при

наличии соответствующих механизмов управления доступом (11.4).

Оборудование, на котором хранится важная и/или критическая коммерческая информация, не следует оставлять без присмотра и, по возможности физически изолировать в надежном месте или использовать специальные защитные устройства на самом оборудовании, чтобы исключить его неавторизованное использование. Должна устанавливаться процедура для случаев кражи или потери мобильных средств связи, принимая во внимание юридические, страховые и другие требования безопасности организации. Переносные устройства необходимо также физически защищать от краж, особенно когда их оставляют без присмотра, забывают, например, в автомобилях или других видах транспорта, гостиничных номерах, конференц-центрах и местах встреч. (9.2.5).

Необходимо информировать сотрудников, использующих переносные устройства о дополнительных рисках и необходимых мероприятиях обеспечения информационной безопасности, связанных с этим способом работы.

Дополнительная информация

Беспроводные соединения сетей с подвижными объектами похожи на другие типы сетевых соединений, но имеют существенные различия, которые должны учитываться при определении средств контроля. Этими различиями являются:

a) некоторые беспроводные протоколы безопасности являются несовершенными и имеют известные слабые места;
b) информация, хранящаяся в переносных компьютерах, иногда не может дублироваться из-за ограниченной полосы пропускания сети и/или оттого, что переносное оборудование невозможно подсоединить в запланированное для дублирования время.

11.7.2 Работа в дистанционном режиме

Определение

Для работы в дистанционном режиме необходимо разработать и реализовать политику, оперативные планы и процедуры.

Руководство по реализации

Организациям следует санкционировать возможность работы в дистанционном режиме только в случае уверенности, что применяются соответствующие меры информационной безопасности, которые согласуются с политикой безопасности организации.

Следует обеспечить необходимую защиту места дистанционной работы от краж оборудования и информации, неавторизованного раскрытия информации, неавторизованного удаленного доступа к внутренним системам организации или неправильного использования оборудования. Важно, чтобы работа в дистанционном режиме была, как авторизована, так и контролируема со стороны руководства, а также был обеспечен соответствующий уровень информационной безопасности этого способа работы.

Нужно рассмотреть следующее:

a) существующую физическую безопасность места работы в дистанционном режиме, с точки зрения безопасности здания и окружающей среды;
b) предлагаемое оборудование места дистанционной работы;
c) требования к безопасности коммуникаций, исходя из потребности в удаленном доступе к внутренним системам организации, важности информации, к которой будет осуществляться доступ, и которая будет передаваться по каналам связи, а также важность самих внутренних систем организации;
d) угрозу неавторизованного доступа к информации или ресурсам со стороны других лиц, имеющих доступ к месту дистанционной работы, например, членов семьи и друзей;
e) использование собственных сетей и требований или ограничений по отноше-

нию к сервисам беспроводных сетей;

f) политики и процедуры предотвращения споров, касающихся прав на интеллектуальную собственность на оборудование, находящееся в частном пользовании;

g) доступ к частному оборудованию (для проверки безопасности машины или во время расследования, который может быть запрещён по законодательству);

h) соглашения по лицензированию программного обеспечения, по которым организации могут стать ответственными за лицензирование программного обеспечения клиентов или рабочих станций, находящихся в частном пользовании работников, подрядчиков или пользователей третьей стороны;

i) антивирусная защита и требования брандмауэров.

Мероприятия по обеспечению информационной безопасности в этих условиях должны включать:

a) обеспечение подходящим оборудованием и мебелью места дистанционной работы;

b) определение видов разрешенной работы, времени работы, классификацию информации, которая может храниться, а также внутренние системы и услуги, доступ к которым авторизовано осуществлять лицо, работающее в дистанционном режиме;

c) обеспечение подходящим телекоммуникационным оборудованием, включая средства обеспечения безопасности удаленного доступа;

d) физическую безопасность;

e) правила и руководства в отношении доступа членов семьи и друзей к оборудованию и информации;

f) обеспечение поддержки и обслуживания оборудования и программного обеспечения;

g) обеспечение страхования;

h) процедуры в отношении резервирования данных и обеспечения непрерывности деятельности;

i) аудит и мониторинг безопасности;

j) аннулирование полномочий, отмену прав доступа и возвращение оборудования, в случае прекращения работы в дистанционном режиме.

При работе в дистанционном режиме применяются коммуникационные технологии, для обеспечения работы сотрудников вне своей организации, в конкретном удаленном месте.

12 Приобретение, усовершенствование и обслуживание информационных систем

12.1 Требования безопасности информационных систем

Цель: обеспечение учета требований безопасности при разработке информационных систем.

Информационные системы включают операционные системы, инфраструктуру, бизнес-приложения, серийных продуктов, сервисы, а также приложения, разработанные пользователями. Процесс проектирования и внедрения бизнес-приложения или сервиса может быть критичными с точки зрения безопасности. Требования к безопасности следует идентифицировать и согласовывать до разработки информационных систем.

Все требования безопасности следует идентифицировать на стадии определения задач проекта, а также обосновывать, согласовывать и документировать в рамках общего

проекта по внедрению информационной системы.

12.1.1 Анализ и детализация требований безопасности

Определение

Необходимо, чтобы в формулировках требований бизнеса в отношении новых информационных систем или усовершенствования существующих систем были учтены требования информационной безопасности.

Руководство по реализации

Необходимо учитывать как встроенные в систему автоматизированные средства обеспечения информационной безопасности, так и необходимость применения организационных мероприятий по управлению информационной безопасностью. Аналогично следует подходить при оценке разработанных или приобретённых пакетов прикладных программ.

Требования безопасности и соответствующие мероприятия по обеспечению информационной безопасности (см. также 7.2) должны учитывать ценность информационных активов, потенциальный ущерб бизнесу, который может стать результатом неэффективности или отсутствия мер безопасности.

Требования по информационной безопасности и процессы реализации безопасности системы должны быть интегрированы на ранних этапах проектирования информационных систем. Средства контроля, введённые на этапе конструирования, реализовать и обслуживать значительно дешевле, чем средства, включённые во время или после реализации.

При закупке продукции необходимо следовать формальному процессу закупки и тестирования. Контракты с поставщиком должны содержать определённые требования безопасности. Там, где функциональные возможности безопасности не удовлетворяют обозначенным требованиям, риск и связанные с ним средства контроля должны быть пересмотрены перед закупкой продукции. Там, где поставляются функциональные дополнительные возможности, что приводит к риску для безопасности, эти возможности должны блокироваться или предлагаемая структура контроля должна быть пересмотрена, чтобы определить, можно ли воспользоваться преимуществом этих дополнительных возможностей.

Дополнительная информация

Как правило, руководство должно требовать использование сертифицированных программных продуктов или продуктов, прошедших независимую оценку. Дальнейшую информацию о критериях оценки продуктов безопасности ИТ можно найти в [9] или других стандартах по оценке или сертификации.

Для определения требований для средств контроля безопасности стандарт [6] предоставляет руководство по процессам управления рисками.

12.2 Правильная обработка приложений

Цель: Предотвращение ошибок, несанкционированного модифицирования или неправильного использования информации в приложениях.

Соответствующие мероприятия по обеспечению информационной безопасности необходимо предусматривать в прикладных системах, включая приложения, написанные самими пользователями, чтобы гарантировать правильную обработку. Эти меры должны также включать обеспечение функциональности подтверждения корректности ввода, обработки и вывода данных.

Дополнительные мероприятия по обеспечению информационной безопасности могут потребоваться для систем, которые обрабатывают, или оказывают воздействие на важные, ценные или критическую информацию, и их необходимо определять на основе

требований безопасности и оценки рисков.

12.2.1 Проверка достоверности входных данных

Определение

Необходимо обращать особое внимание на корректность входных данных для прикладных систем.

Руководство по реализации

При вводе бизнес-транзакций, постоянных данных (имена и адреса, кредитные лимиты, идентификационные номера клиентов) и таблиц параметров (цены продаж, курсы валют, ставки налогов) следует применять проверку корректности ввода для обеспечения уверенности в их соответствии исходным данным. Для этого целесообразно применение следующих мероприятий по обеспечению информационной безопасности:

a) проверки исключения двойного ввода или другие проверки ввода, такие как проверка границы или полей ограничения входных данных, с целью обнаружения следующих ошибок:
   1) значений, выходящих за допустимый диапазон;
   2) недопустимых символов в полях данных;
   3) отсутствующие или неполные данные;
   4) превышение верхних и нижних пределов объема данных;
   5) неавторизованные или противоречивые контрольные данные;
b) периодический анализ (просмотр) содержимого ключевых полей или файлов данных для подтверждения их достоверности и целостности;
c) сверка твердых (печатных) копий вводимых документов с вводимыми данными на предмет выявления любых неавторизованных изменений вводимых данных (необходимо, чтобы все изменения во вводимых документах были авторизованы);
d) процедуры реагирования на ошибки, связанные с подтверждением данных;
e) процедуры проверки правдоподобия вводимых данных;
f) определение обязанностей всех сотрудников, вовлеченных в процесс ввода данных;
g) создание журнала действий, вовлечённых в процесс ввода данных (см. 10.10.1).

Дополнительная информация

Можно рассмотреть и автоматическую проверку входных данных для снижения риска ошибок и предотвращения стандартных атак, включая переполнение буфера и введение кода.

12.2.2 Контроль внутренней обработки

Определение

С целью обнаружения искажений информации, посредством ошибок обработки или умышленных действий, в функции прикладных систем следует включать возможности, обеспечивающие выполнение контрольных проверок.

Руководство по реализации

Необходимо, чтобы дизайн и реализация приложений обеспечивали уверенность в том, что внедрены ограничения, направленные на минимизацию риска отказов, ведущих к потере целостности данных. Необходимо учитывать, в частности, следующее:

a) использование функций добавления, модификации и удаления данных, чтобы внедрить изменения в данных;
b) процедуры для предотвращения выполнения программ в неправильной последовательности или исполнения после сбоя на предыдущем этапе обработки

данных (10.1.1);

c) использование корректирующих программ для восстановления после сбоев и обеспечения правильной обработки данных;

d) защиту от атак, применяющих перегрузки/переполнения.

Должен быть подготовлен список проверок, действия задокументированы, а результаты должны храниться в безопасном месте. Примером таких проверок могут быть следующие:

a) средства контроля сеансовой или пакетной обработки с целью выверки контрольных данных (остатков/контрольных сумм) в файлах данных после транзакционных обновлений;

b) средства контроля входящих остатков с целью проверки входящих остатков с предыдущими закрытыми остатками, а именно:

1) средства контроля "от выполнения-к-выполнению";
2) общие суммы измененных данных в файле;
3) средства контроля "от программы-к-программе";

c) подтверждение корректности данных, генерированных системой (12.2.1);

d) проверки целостности, аутентичности или другого параметра безопасности полученных или переданных данных (программного обеспечения) между центральным и удаленными компьютерами;

e) контрольные суммы записей и файлов;

f) проверки для обеспечения уверенности в том, что прикладные программы выполняются в нужное время;

g) проверки для обеспечения уверенности в том, что программы выполняются в правильном порядке и прекращают работу в случае отказа, и что дальнейшая обработка приостанавливается до тех пор, пока проблема не будет разрешена;

h) создание журнала регистрации действий, участвовавших в обработке (см. 10.10.1).

Дополнительная информация

Правильно введённые данные могут быть искажены ошибкам аппаратного обеспечения, ошибками при обработке или в результате намеренных действий. Проверки достоверности будут зависеть от характера приложения и воздействия любой порчи данных на деловую деятельность.

12.2.3 Целостность сообщений

Определение

Необходимо обеспечить аутентичность и защиту целостности сообщений в приложениях, а также определить, реализовать соответствующие средства контроля.

Руководство по реализации

Для определения необходимости целостности сообщений и для определения наиболее пригодного метода реализации должна приводиться оценка рисков безопасности.

Дополнительная информация

В качестве подходящего средства реализации аутентификации сообщений могут использоваться криптографические методы (см. 12.3)

12.2.4 Проверка достоверности выходных данных

Определение

Данные, выводимые из прикладной системы, необходимо проверять на корректность, чтобы обеспечивать уверенность в том, что обработка информации выполнена правильно.

Руководство по реализации

Подтверждение корректности данных вывода может включать:

a) проверки на правдоподобие с целью определения, являются ли выходные данные приемлемыми;
b) выверки контрольных счетчиков на предмет удостоверения, что все данные были обработаны;
c) обеспечение достаточной информации для получателя результатов вывода или последующей системы обработки, чтобы определить корректность, законченность, точность и классификацию информации;
d) процедуры по выполнению тестов на подтверждение выводимых данных;
e) определение обязанностей всех сотрудников, вовлеченных в процесс вывода данных.
f) создание журнала действий в процессе проверки достоверности выходных данных.

Дополнительная информация

Как правило, системы и прикладные системы построены на допущении, что при наличии соответствующих подтверждений корректности, проверок и тестирования, выводимые данные будут всегда правильны. Однако, это допущение не всегда верно; т.е. системы, которые были протестированы, ещё могут производить некорректные выходы по некоторым обстоятельствам.

12.3 Криптографические средства контроля

Цель: защита конфиденциальности, аутентичности или целостности информации криптографическими средствами.

Необходимо разработать политику использования криптографических средств контроля. Для поддержки использования криптографических методов должно быть в наличии распределение ключей.

12.3.1 Политика использования криптографических средств контроля

Определение

Необходимо разработать и реализовать политику использования криптографических средств контроля для защиты информации.

Руководство по реализации

При разработке криптографической политики необходимо учитывать следующее:

a) методику использования криптографических средств во всей организации, включая общие принципы, в соответствии с которыми будет защищаться служебная информация (см. также 5.1.1);
b) на основе оценки риска необходимо определить необходимый уровень защиты, учитывая тип, стойкость и качество алгоритма шифрования;
c) применение шифрования для защиты секретной информации, передаваемой переносными или съёмными носителями информации, устройствами или через линии связи;
d) принципы управления ключами, включая методы восстановления зашифрованной информации, связанные с защитой криптографических ключей в случае потери, компрометации или повреждении ключей;
e) роли и обязанности должностных лиц за:
   1) реализацию политики;
   2) управление ключами, включая образование ключей (см. также 12.3.2);
f) перечень мероприятий, которые должны обеспечить эффективность внедрения криптозащиты во всей организации;

g) воздействие применения зашифрованной информации на средства контроля, которые зависят от проверки содержания (например, обнаружение вируса).

При реализации криптографической политики организации необходимо рассмотреть правила и национальные ограничения, которые могут налагаться на применение криптографических методов в различных частях мира, и проблемы пересечения границ потоком зашифрованной информации (см. также 15.1.6).

Для достижения различных целей безопасности можно использовать различные криптографические средства защиты; например:

a) конфиденциальность: применение шифрования информации для защиты секретной или критической информации, хранимой или передаваемой;
b) целостность/аутентичность: применение цифровых подписей или кодов аутентификации сообщений для защиты аутентичности и целостности хранимой или передаваемой критической информации;
c) невозможность отказа: применение криптографических методов для получения доказательства появления или отсутствия события или действия.

Дополнительная информация

Решения относительно применения криптографической защиты следует рассматривать в рамках более общего процесса оценки рисков и выбора мероприятий по обеспечению информационной безопасности. Для определения необходимого уровня защиты информации следует провести оценку рисков, которая должна использоваться для определения того, является ли криптографическое средство подходящим, какой тип средств необходим, с какой целью и в отношении каких бизнес-процессов.

Политика использования криптографических средств контроля необходима для получения максимальной выгоды и сведения к минимуму рисков использования криптографических методов, а также для избежания несоответствующего или неправильного использования. При использовании цифровых подписей необходимо учитывать любое релевантное законодательство, определяющее условия, по которым цифровая подпись является обязательной по закону (см. также 15.1).

Необходимо получить консультацию специалиста по определению соответствующего уровня защиты и подходящих спецификаций, которые обеспечат требуемую защиту и поддержку безопасной системы распределения ключа (см. также 12.3.2).

Комитет ISO/IEC JTC1 SC27 разработал несколько стандартов, связанных с криптографическими средствами контроля. Дальнейшую информацию можно также найти в [10] и [11].

12.3.2 Распределение ключей

Определение

Следует применять систему защиты для обеспечения использования организацией криптографических методов.

Руководство по реализации

Криптографические ключи необходимо защищать от изменения, потери и разрушения. Кроме того, секретным и личным ключам необходима защита от несанкционированного раскрытия.

Необходимо, чтобы система обеспечения безопасности использования ключей основывалась на согласованном множестве способе, процедур и безопасных методов для:

a) генерации ключей для различных криптографических систем и различных приложений;
b) генерации и получения сертификатов открытых ключей;
c) рассылки ключей предназначенным пользователям, включая инструкции по их активации при получении;

d) хранения ключей; при этом необходимо наличие инструкции авторизованным пользователям для получения доступа к ключам;
e) смены или обновления ключей, включая правила порядка и сроков смены ключей;
f) порядка действий в отношении скомпрометированных ключей;
g) аннулирования ключей, в том числе, способы изъятия или деактивизации ключей, если ключи были скомпрометированы или пользователь уволился из организации (в этом случае ключи необходимо архивировать);
h) восстановления ключей, которые были утеряны или испорчены для рассекречивания зашифрованной информации;
i) архивирования ключей, например, для архивированной или резервной информации;
j) разрушения ключей;
k) регистрации и аудита действий, связанных с управлением ключами.

Для уменьшения вероятности компрометации необходимо, чтобы ключи имели определенные даты активизации и деактивизации, чтобы их можно было бы использовать в течение ограниченного периода времени, который зависит от обстоятельств использования криптографических средств контроля, и от степени риска раскрытия информации.

Этот процесс аутентификации можно осуществить, используя сертификаты ключей, которые обычно выдаются сертификационным органом, который должен быть признанной организацией с соответствующими средствами контроля и процедурами, обеспечивающими требуемый уровень доверия.

Необходимо, чтобы содержание соглашений с внешними поставщиками криптографических сервисов, например, с органом сертификации, включало вопросы ответственности, надежности сервисов и времени реагирования на запросы по их предоставлению (6.2.3).

Дополнительная информация

Распределение криптографических ключей необходимо для эффективного использования криптографических методов. В стандарте [12] предоставляется дополнительная информация по распределению ключей. Двумя криптографическими методами являются:

a) методы в отношении секретных ключей, где две или более стороны совместно используют один и тот же ключ, и этот ключ применяется как для шифрования, так и дешифрования информации. Этот ключ должен храниться в секрете, так как любой, имеющий доступ к этому ключу, может дешифровать всю информацию, зашифрованную с помощью этого ключа, или ввести несанкционированную информацию, используя ключ;
b) методы в отношении открытых ключей, где каждый пользователь имеет пару ключей, открытый ключ (который может быть показан любому) и личный ключ (который должен храниться в секрете). Методы с открытыми ключами могут использоваться для шифрования и для генерации цифровых подписей (см. также [13], [14], [15]).

Существует угроза подделки цифровой подписи посредством замены её открытым ключом пользователя. Эту проблему можно разрешить применением сертификата открытого ключа.

Криптографические методы могут также использоваться для защиты криптографических ключей. Может потребоваться наличие процедур обработки юридических запросов, касающихся доступа к криптографическим ключам, например, чтобы зашифрованная информация стала доступной в незашифрованной форме, для доказательств в суде.

12.4 Безопасность системных файлов

Цель: Обеспечение безопасности системных файлов.

Доступ к системным файлам и исходному коду программы должен контролироваться, а проекты ИТ и вспомогательные действия проводиться безопасным образом. Необходимо соблюдать осторожность во избежание показа секретных данных в испытательной среде.

12.4.1 Контроль за операционным программным обеспечением

Определение

В наличии должны быть процедуры контроля установки программного обеспечения в операционные системы.

Руководство по реализации

Для сведения к минимуму риска нарушений в операционных системах, для контроля изменений необходимо соблюдать следующие правила:

a) обновление библиотек программного обеспечения, приложений и программ следует выполнять только обученными администраторами при наличие соответствующей авторизации руководства (12.4.3);
b) системы, находящейся в промышленной эксплуатации, должны состоять только из исполнимых программных кодов, а не кода разработки или компилятора;
c) приложения и программное обеспечение операционной системы должны реализовываться только после объёмного и успешного тестирования; тесты должны включать испытания на применимость, безопасность, воздействие на другие системы и удобство для пользователя и проводиться на отдельных системах (см. также 10.1.4); необходимо обеспечить обновление всех соответствующих библиотек исходных модулей программы;
d) для поддержания контроля за всем реализованным программным обеспечением, а также системной документацией, должна применяться система контроля конфигурации;
e) стратегия возврата должна быть в наличии до реализации изменений;
f) необходимо, чтобы журнал аудита поддерживал все обновления библиотек программ находящихся в промышленной эксплуатации;
g) предыдущие версии прикладного программного обеспечения следует сохранять для восстановления системы в случае непредвиденных обстоятельств;
h) старые версии программного обеспечения должны архивироваться вместе со всей требуемой информацией и параметрами, процедурами, подробностями конфигурации и вспомогательным программным обеспечением столь же долго, сколько данные остаются в архиве.

Необходимо, чтобы программное обеспечение, используемое в промышленной эксплуатации, поддерживалось на уровне, обеспечивающем поддержку разработчика. Со временем продавцы перестанут поддерживать старые версии программного обеспечения. Организация должна учитывать риски опоры на использование неподдерживаемого программного обеспечения.

При любом решении провести обновление до уровня новой версии следует принимать во внимание безопасность версии, то есть, новые функциональные возможности обеспечения информационной безопасности, или наличие и серьезность проблем безопасности, связанных с этой версией. Целесообразно использовать программные патчи (исправления), если они могут закрыть или снизить угрозы безопасности (см. также 12.6.1).

Физический или логический доступ предоставляется поставщикам (разработчикам), по мере необходимости, только для целей поддержки программного обеспечения при на-

личии разрешения руководства. При этом действия поставщика (разработчика) должны контролироваться.

Компьютерное программное обеспечение может основываться на поставляемом извне программном обеспечении, которое должно управляться и контролироваться в целях избежания несанкционированных изменений, которые могут создать слабые места в системе безопасности.

Дополнительная информация

Операционная система обновляется только по необходимости, например, если действующая версия операционной системы больше не соответствует бизнес-требованиям. Усовершенствования не должны проводиться только потому, что существует новая версия системы. Просто новые версии могут быть менее безопасными, менее стабильными и менее понятными, чем действующие системы.

12.4.2 Защита данных системных испытаний

Определение

Данные испытаний должны тщательно отбираться, защищаться и контролироваться.

Руководство по реализации

Следует избегать использования баз данных, находящихся в промышленной эксплуатации и содержащих личную информацию или любую другую важную информацию с целью тестирования. Если подобная информация используется, то нужно удалить или модифицировать до неузнаваемости все секретные детали и содержимое перед использованием. Для защиты операционных данных, когда они используются для целей тестирования, необходимо применять следующие мероприятия по обеспечению информационной безопасности:

a) процедуры контроля доступа, применяемые для прикладных систем находящихся в промышленной эксплуатации, следует также применять и к прикладным системам в среде тестирования;
b) при каждом копировании операционной информации для прикладной системы тестирования предусматривать авторизацию этих действий;
c) после того, как тестирование завершено, операционную информацию следует немедленно удалить из прикладной системы среды тестирования;
d) копирование и использование операционной информации необходимо регистрировать в журнале аудита.

Дополнительная информация

Для осуществления системного и приемочного тестирования обычно требуется существенные объемы тестовых данных, которые максимально приближены к операционным данным.

12.4.3 Контроль доступа к исходному коду программы

Определение

Доступ к исходному коду программы должен быть ограниченным.

Руководство по реализации

Доступ к исходному коду программы и связанные с ним компоненты (такие как: проекты, спецификации, планы верификации и проверок достоверности) должны строго контролироваться для предотвращения использования несанкционированных функций и для избежания непреднамеренных изменений. По отношению к исходному коду программы этого можно достичь путём контролируемого централизованного хранения такого кода, предпочтительно в библиотеках исходных модулей программы. Для контроля доступа к таким библиотекам с целью уменьшения возможности разрушения компьютерных программ необходимо рассмотреть следующие правила (см. также раздел 11):

a) по возможности, исходные библиотеки программ следует хранить отдельно от бизнес-приложений, находящихся в промышленной эксплуатации;
b) исходный код программы и библиотеки исходных модулей программы должны управляться в соответствии с установленными процедурами;
c) персоналу поддержки информационных технологий не следует предоставлять неограниченный доступ к исходным библиотекам программ;
d) обновление библиотек и обеспечение программистов исходными текстами следует осуществлять только назначенному библиотекарю после авторизации, полученной от менеджера, отвечающего за поддержку конкретного бизнес-приложения;
e) листинги программ следует хранить в безопасным образом (10.7.4);
f) следует вести журнал аудита для всех доступов к исходным библиотекам;
g) поддержку и копирование исходных библиотек следует проводить под строгим контролем с целью предотвращения внесения неавторизованных изменений (12.5.1).

Дополнительная информация

Исходным кодом программы является записанный программистами код, который скомпилирован для создания исполняемых файлов. Некоторые языки программирования формально не делают различия между исходным кодом и исполняемыми файлами, поскольку эти файлы создаются во время их активации.

Дальнейшая информация по управлению конфигурациями и процессу жизненного цикла программного обеспечения представлена в стандартах [16] и [17].

12.5 Безопасность в процессах разработки и поддержки

Цель: поддержание безопасности прикладных систем и информации.

Необходимо, чтобы менеджеры, ответственные за прикладные системы, также были ответственны и за безопасность среды проектирования или поддержки. Они должны обеспечивать уверенность в том, что все предложенные изменения системы проанализированы на предмет возможной компрометации безопасности, как системы, так и среды промышленной эксплуатации.

12.5.1 Процессы контроля изменений

Определение

Реализация изменений должна контролироваться применением формальных процедур контроля изменений.

Руководство по реализации

Формальные процедуры контроля изменений должны документироваться и осуществляться с целью сведения к минимуму искажения информационных систем. Внедрение новых систем и значительные изменения в существующих системах должны осуществляться в ходе формального процесса документирования, создания спецификаций, тестирования, контроля качества и управляемой реализации.

Этот процесс должен включать оценку риска, анализ воздействий изменений и спецификаций нужных средств контроля безопасности. Этот процесс должен также обеспечивать отсутствие риска для существующих процедур обеспечения безопасности и контроля, предоставление оказывающим помощь программистам доступ только к тем частям системы, которые необходимы для их работы и получение формального согласия и утверждения любого изменения.

Там, где это возможно, следует объединять меры по обеспечению информационной безопасности используемых бизнес-приложений и изменений в прикладных программах

(см. также 10.1.2). Необходимо, чтобы этот процесс включал:

a) обеспечение протоколирования согласованных уровней авторизации;
b) обеспечение уверенности в том, что запросы на изменения исходят от авторизованных соответствующим образом пользователей;
c) анализ мер информационной безопасности и процедур, обеспечивающих целостность используемых систем для обеспечения уверенности в том, что они не будут скомпрометированы изменениями;
d) идентификацию всего программного обеспечения, информации, объектов баз данных и также аппаратных средств, требующих изменений;
e) получение формализованного одобрения детальных запросов/предложений на изменения перед началом работы;
f) обеспечение того, чтобы авторизованный пользователь одобрил все изменения до начала их реализации;
g) обеспечение того, чтобы комплект системной документации обновлялся после завершения каждого изменения, и чтобы старая документация архивировалась или утилизировалась;
h) поддержку контроля версий для всех обновлений программного обеспечения;
i) регистрацию в журналах аудита всех запросов на изменение;
j) коррекцию эксплуатационной документации (10.1.1) и пользовательских процедур в соответствии с внесенными изменениями;
k) осуществление процесса внедрения изменений в согласованное время без нарушения затрагиваемых бизнес процессов.

Дополнительная информация

Изменение программного обеспечения может повлиять на операционную среду.

Хорошей практикой является испытание нового программного обеспечения в среде, отделённой от производственной среды и среды разработок (см. также 10.1.4). Это обеспечивает средство контролирования нового программного обеспечения и позволяет осуществить дополнительную защиту оперативной информации, применяемой для испытаний. При этом подразумевается внедрение заплат, служебных пакетов и других усовершенствований. В критических системах не должны использоваться автоматические корректировки, поскольку некоторые из них могут вызвать сбои в критических приложениях (см. 12.6).

12.5.2 Технический пересмотр приложений после внесения изменений в операционных системах

Определение

При изменении операционных систем критические бизнес-приложения должны пересматриваться и испытываться для проверки отсутствия вредного воздействия на операции или безопасность организации

Руководство по реализации

Этот процесс должен включать:

a) анализ средств контроля бизнес-приложений и процедур целостности, чтобы обеспечивать уверенность в том, что они не были скомпрометированы изменениями операционной системы;
b) обеспечение уверенности в том, что ежегодный план поддержки и бюджет предусматривают анализ и тестирование систем, необходимые при изменениях операционной системы;
c) обеспечение своевременного поступления уведомлений об изменениях операционной системы для возможности проведения соответствующего теста и анализа их влияния на информационную безопасность перед установкой измене-

ний в операционную систему;

d) контроль документирования соответствующих изменений в планах обеспечения непрерывности бизнеса (раздел 14).

Специальную группу или отдельное лицо необходимо сделать ответственным за управление уязвимостями и выпуском продавцом заплат и исправлений (см.12.6)

12.5.3 Ограничения для изменений в пакетах программного обеспечения

Определение

Модификаций в пакетах программного обеспечения нужно избегать, ограничиваясь необходимыми изменениями, а все внесённые изменения должны строго контролироваться.

Руководство по реализации

Насколько возможно и допустимо с практической точки зрения, поставляемые поставщиком пакеты программ следует использовать без внесения изменений. При необходимости модифицирования пакета программного обеспечения нужно учесть следующие пункты:

a) риск компрометации встроенных средств контроля и процесса обеспечения целостности;

b) необходимость получения согласия поставщика;

c) возможность получения требуемых изменений от поставщика в виде стандартного обновления программ;

d) необходимость разработки дополнительных мер поддержки программного обеспечения, если организация в результате внесенных изменений станет ответственной за будущее сопровождение программного обеспечения.

В случае существенных изменений оригинальное программное обеспечение следует сохранять, а изменения следует вносить в четко идентифицированную копию. Процесс обновления программного обеспечения должен быть реализован для обеспечения установки большинства утверждённых самых современных заплат и корректировок приложений в санкционированное программное обеспечение (см. 12.6). Все изменения должны быть полностью протестированы, чтобы их при необходимости можно было применить для будущих обновлений программного обеспечения. По требованию модификации должны тестироваться и подтверждаться оценочным органом.

12.5.4 Утечка информации

Определение

Необходимо предотвратить возможности утечки информации.

Руководство по реализации

Для ограничения риска утечки информации, например, посредством использования тайных каналов необходимо рассмотреть следующее:

a) поиск скрытой информации в посторонних носителях информации и средствах связи;

b) маскирование и модулирование поведения систем и средств связи для уменьшения вероятности извлечения третьей стороной информации из такого поведения;

c) использование систем и программного обеспечения, которые, как считается, имеют высокую степень целостности, например, использование оценённой продукции (см. [9]);

d) постоянный мониторинг действий персонала и систем, где это разрешено существующим законодательством и правовыми нормами;

e) мониторинг использования ресурсов в компьютерных системах.

Дополнительная информация

Тайными каналами являются каналы, которые не предназначены для проведения информационных потоков, но которые могут, тем не менее, присутствовать в системе или сети. Например, манипулирование битами в пакетах протокольных программ связи может использоваться как скрытый способ сигнализации. По своему характеру, предотвращение существования всех возможных тайных каналов очень затруднено, если не невозможно. Однако, такие каналы часто задействуются троянскими кодами (см. также 10.4.1). Следовательно, принятие мер защиты от троянского кода снижает риск использования тайных каналов.

Предотвращение несанкционированного доступа к сети (11.4), а также политики и процедуры, препятствующие персоналу неправильно использовать информационные службы (15.1.5) помогают осуществлять защиту от тайных каналов.

12.5.5 Разработка программного обеспечения с привлечением посторонних организаций

Определение

Разработка программного обеспечения с привлечением посторонних организаций должна находиться под наблюдением и контролем вашей организации.

Руководство по реализации

В случаях, когда для разработки программного обеспечения привлекается сторонняя организация, необходимо применять следующие меры обеспечения информационной безопасности:

a) осуществлять контроль наличия лицензионных соглашений, определенности в вопросах собственности на программы и прав интеллектуальной собственности (15.1.2);
b) сертификацию качества и правильности выполненных работ;
c) заключение "escrow" соглашения, предусматривающих депонирование исходного текста на случай невозможности третьей стороны выполнять свои обязательства;
d) обеспечение прав доступа для аудита с целью проверки качества и точности выполненной работы;
e) документирование требований к качеству и функциональности безопасности программ в договорной форме;
f) тестирование перед установкой программ на предмет обнаружения "Троянов" и вредоносных кодов.

12.6 Управление техническими уязвимостями

Цель: Снижение рисков, вытекающих из использования технических уязвимостей

Управление техническими уязвимостями должно быть осуществлено эффективным, систематическим и воспроизводимым путём с измерениями, предназначенными для подтверждения его эффективности. Эти предпосылки должны включать операционные системы и любые другие применяемые приложения.

12.6.1 Контроль технических уязвимостей

Определение

Необходимым являются получение своевременной информации о технических уязвимостях используемых информационных систем, оценка подвергания организации подобным уязвимостям и принятие соответствующих мер по устранению связанных с ними рисков.

Руководство по реализации

Текущая полная инвентаризация активов (см. 7.1) является предпосылкой эффективного управления техническими уязвимостями. Специфическая информация, требуемая для поддержки управления техническими уязвимостями, включает продавца программного обеспечения, номера версий, текущее состояние развёртывания (например, какое программное обеспечение установлено в какой системе) и лицо (лица) внутри организации, ответственные за программное обеспечение.

В ответ на обнаружение потенциальных технических уязвимостей должны предприниматься соответствующие своевременные действия. Для выработки эффективного процесса управления техническими уязвимостями надо следовать следующему руководству:

a) организация должна определить и установить роли и обязанности, связанные с управлением техническими уязвимостями, включая мониторинг уязвимостей, оценку риска уязвимостей, наложений заплат, прослеживание активов и любые обязанности, требуемые для координации;

b) информационные ресурсы, которые будут использоваться для определения релевантных технических уязвимостей и для поддержания осведомлённости о них, должны быть определены для программного обеспечения и другой технологии (основанной на списке инвентаризации активов, см. 7.1.1); эти информационные ресурсы должны обновляться на основе изменений в инвентаризации или при обнаружении других новых или полезных ресурсов;

c) для реагирования на извещения о потенциальных технических уязвимостях должна быть определена временная последовательность;

d) после обнаружения потенциальной технической уязвимости организация должна определить связанные с ней риски и действия, которые надо предпринять; такие действия должны включать наложение заплат на уязвимые системы и/или применение других средств контроля;

e) в зависимости от того, как срочно надо отреагировать на техническую уязвимость, необходимо осуществить действия, соответствующие средствам контроля, которые связаны с управлением внесения изменений (см. 12.5.1), или выполняя процедуры реагирования на инцидент нарушения информационной безопасности (см. 13.2);

f) при наличии заплаты необходимо оценить риски, связанные с её установкой (риски, обусловленные уязвимостью, надо сравнивать с риском установки заплаты);

g) перед установкой заплат последние должны пройти тест на эффективность и на то, что их установка не приведёт к появлению побочных эффектов, которые не являются допустимыми; если заплата отсутствует, необходимо рассмотреть средства контроля, как:
   1) отключение сервисов или возможностей, связанных с уязвимостью;
   2) адаптирование или добавление средств контроля доступа, например, брандмауэров на границах сетей (см. 11.4.5);
   3) усиленный мониторинг для обнаружения или предотвращения фактических атак;
   4) повышение осведомлённости об уязвимости;

h) по всем осуществлённым процедурам необходимо вести контрольный журнал;

i) процесс управления техническими уязвимостями необходимо постоянно контролировать и оценивать для обеспечения его эффективности;

j) в первую очередь должны рассматриваться системы с высокой степенью риска.

Дополнительная информация

Правильное функционирование процесса управления техническими уязвимостями имеет большое значение для многих организаций и, следовательно, должен постоянно контролироваться. Для определения потенциально релевантных технических уязвимостей необходимо вести точную инвентаризацию.

Управление техническими уязвимостями можно рассматривать как подфункцию управления внесения изменений и, как таковая, может использовать преимущества процессов и процедур управления внесения изменений (см. 10.1.2 и 12.5.1).

Продавцы часто находятся под значительным давлением выпускать заплаты как можно скорее. Это может привести к неадекватному решению проблемы с помощью заплаты, и её применение может привести к негативным побочным эффектам. Также в некоторых случаях установку заплаты трудно осуществить, поскольку там уже стоит заплата.

Если адекватное тестирование заплат невозможно, например, из-за больших затрат или отсутствия ресурсов, задержку в положении заплат можно использовать для оценки связанных с ними рисков на основе опыта других пользователей.

13 Управление инцидентами нарушения информационной безопасности

13.1 Сообщение о нарушениях и слабых местах информационной безопасности

Цель: Обеспечение передачи сообщений о случаях и слабых местах информационной безопасности, связанных с информационными системами, способом, позволяющим своевременно предпринимать корректирующие действия.

Необходимо иметь формальные процедуры сообщения о событиях и их эскалации. Все сотрудники, подрядчики и пользователи третьей стороны должны быть осведомлены о процедурах сообщения о различных типах событий и слабых местах, которые могут повлиять на безопасность активов организации. От них необходимо требовать сообщать как можно быстрее о любых событиях и слабых местах информационной безопасности определенному контактному лицу.

13.1.1 Сообщение о событиях нарушения информационной безопасности

Определение

О событиях информационной безопасности следует незамедлительно сообщать через административные каналы.

Руководство по реализации

Необходимо внедрить формализованную процедуру информирования об инцидентах нарушения информационной безопасности, а также процедуру реагирования на инциденты и процедуру эскалации, устанавливающие действия, которые должны быть предприняты после получения сообщения об инциденте нарушения информационной безопасности. Для сообщения о событиях нарушения информационной безопасности должно быть установлено место контакта. Необходимо, чтобы это место контакта было известно всему персоналу организации, было всегда доступно, и оттуда всегда могла последовать адекватная и своевременная реакция.

Все сотрудники, подрядчики и пользователи третьей стороны должны быть ознакомлены с процедурой информирования об инцидентах нарушения информационной безопасности, а также проинформированы о необходимости незамедлительного сообщения об инцидентах. Они также должны быть осведомлены о процедуре сообщения о случаях нарушения информационной безопасности и месте контакта. Процедуры сообщения должны включать:

а) подходящие процессы обратной связи, обеспечивающие уведомление лиц, сообщивших о случаях нарушения, о результатах работы с этими случаями после

закрытия дела;

b) формы сообщения о случаях нарушения информационной безопасности, чтобы оказать помощь сообщающему лицу запомнить все необходимые действия в случае нарушения информационной безопасности;

c) правильное поведение в случае нарушения информационной безопасности, т.е.:
   1) немедленное оповещение о всех существенных деталях (например, типе несоответствия или нарушения, возникновениях неправильных срабатываний, появлении сообщений на экране, странное поведение);
   2) неприменение каких-либо действий кроме немедленного сообщения в место контакта;

d) ссылки на формальный дисциплинарный процесс при работе с сотрудниками, подрядчиками и пользователями третьей стороны, совершающими нарушения безопасности.

В средах с высокой степенью риска может предусматриваться сигнализация о принуждении*, где лицо под принуждением может указать на подобные проблемы. Процедуры реагирования на сигналы принуждения должны отражать ситуации с высокой степенью риска, на которую указывают эти сигналы.

Дополнительная информация

Примерами случаев и инцидентов нарушения информационной безопасности являются:

a) потеря сервиса, оборудования или средств обработки информации;
b) неправильное срабатывание или перегрузки системы;
c) ошибки оператора;
d) несоблюдение политик или руководств;
e) нарушение физических мер обеспечения безопасности;
f) неконтролируемое внесение изменений в систему;
g) неправильное срабатывание программного или аппаратного обеспечения;
h) нарушения доступа.

При должном внимании к аспектам конфиденциальности инциденты нарушения информационной безопасности могут использоваться в обучении пользователей (см. 8.2.2) как примеры того, что может произойти, как реагировать на подобные инциденты и как избежать их в будущем. Для правильного реагирования на случаи и инциденты нарушения информационной безопасности может стать обязательным сбор свидетельств после их появления (см. 13.2.3).

Неправильное срабатывание или другое аномальное поведение системы может стать индикатором атаки на безопасность или нарушения безопасности, и о них надо всегда докладывать как о случае нарушения информационной безопасности.

Дополнительную информацию о сообщении о случаях нарушения информационной безопасности и управлении инцидентами нарушения информационной безопасности можно найти в стандарте [3].

13.1.2 Сообщение о слабых местах безопасности

Определение

От всех сотрудников, подрядчиков и пользователей третьей стороны необходимо требовать, чтобы они обращали внимание и сообщали о любых замеченных или предполагаемых недостатках в области безопасности в системах или сервисах.

Руководство по реализации

* Сигнализация о принуждении – это способ, с помощью которого можно незаметно показать, что действие совершается «под принуждением».

Все сотрудники, подрядчики и пользователи третьей стороны должны как можно скорее сообщать о подобных случаях или своему начальству, или непосредственно поставщику услуг с целью предотвращения инцидентов нарушения информационной безопасности. Механизм сообщения должен быть простым, доступным и всегда в наличии. Они должны быть информированы, что они не должны ни при каких обстоятельствах самостоятельно искать подтверждения подозреваемому недостатку в системе безопасности.

Дополнительная информация

Надо советовать сотрудникам, подрядчикам и пользователям третьей стороны не пытаться использовать предполагаемые слабые места безопасности. Испытание слабых мест может быть воспринято как потенциальное неправильное использование системы и может нанести ущерб информационной системе или службе, а также может привести лицо, проводящее испытание, к судебной ответственности.

13.2 Управление инцидентами нарушения информационной безопасности и их усовершенствование

Цель: Обеспечение последовательного и эффективного подхода к управлению инцидентами нарушения информационной безопасности.

Для эффективной работы со случаями нарушения информационной безопасности и слабыми местами безопасности после того, как о них поступило сообщение, должны быть в наличии обязанности и процедуры. Для мониторинга, оценки общего управления инцидентами нарушения информационной безопасности и реагирования на них должен использоваться процесс непрерывного усовершенствования.

Там, где требуются свидетельства, они должны быть собраны для обеспечения соответствия правовым требованиям.

13.2.1 Обязанности и процедуры

Определение

Для обеспечения быстрого, эффективного и правильного реагирования на инциденты нарушения информационной безопасности необходимо выработать административные обязанности и процедуры.

Руководство по реализации

Кроме сообщений о случаях нарушения и слабых местах информационной безопасности для обнаружения инцидентов нарушения информационной безопасности должен применяться мониторинг систем, предупреждений и уязвимостей (10.10.2). Для процедур управления инцидентами нарушения информационной безопасности должны рассматриваться следующие правила:

a) для работы с различными типами инцидентов необходимо установить следующие процедуры:
   1) сбои информационных систем и утрата сервисов;
   2) вредоносный код (см. 10.4.1);
   3) отказ в обслуживании;
   4) ошибки вследствие неполных или неточных данных;
   5) нарушения конфиденциальности и целостности;
   6) неправильное использование информационных систем;
b) дополнение к обычным планам обеспечения непрерывности (см. 14.1.3), должны существовать процедуры касательно (13.2.2):
   1) анализа и идентификации причины инцидента;
   2) локализации;
   3) планирования и внедрения средств, предотвращающих повторное проявление

инцидентов, при необходимости;

4) взаимодействия с лицами, на которых инцидент оказал воздействие, или участвующих в устранении последствий инцидента;
5) информирования о действиях соответствующих должностных лиц;

c) журналы аудита и аналогичные свидетельства должны быть собраны (13.2.3) и защищены соответствующим образом, с целью:
1) внутреннего анализа проблемы;
2) использования как доказательство в отношении возможного нарушения условий контракта, нарушения требований законодательства или, в случае гражданских или уголовных судебных разбирательств, касающихся, например, защиты персональных данных или неправомочного использования компьютеров;
3) ведения переговоров относительно компенсации ущерба с поставщиками программного обеспечения и услуг;

d) действия по устранению сбоев систем и ликвидации последствий инцидентов нарушения информационной безопасности должны быть под тщательным и формализованным контролем. Необходимо наличие процедур с целью обеспечения уверенности в том, что:
1) только полностью идентифицированному и авторизованному персоналу предоставлен доступ к системам и данным в среде промышленной эксплуатации (6.2 в отношении доступа третьей стороны);
2) все действия, предпринятые при чрезвычайных обстоятельствах, подробно документально оформлены;
3) о действиях, предпринятых при чрезвычайных обстоятельствах, сообщено руководству организации, и они проанализированы в установленном порядке;
4) целостность бизнес-систем и систем контроля подтверждена в минимальные сроки.

Цели управления инцидентами нарушения информационной безопасности должны быть согласованы с руководством и лица, ответственные за управление инцидентами, должны знать приоритеты организации при работе с инцидентами нарушения информационной безопасности.

Дополнительная информация

Инциденты нарушения информационной безопасности могут выходить за границы организации и национальные границы. Для правильного реагирования на них необходимо координировать ответные действия и совместно использовать информацию об инцидентах с посторонними организациями.

13.2.2 Извлечение уроков из инцидентов нарушения информационной безопасности

Определение

Необходимо установить порядок мониторинга и регистрации инцидентов в отношении их количества, типов, параметров, а также связанных затрат.

Руководство по реализации

Информация, полученная из оценки инцидентов нарушения информационной безопасности, должна применяться для идентификации повторяющихся инцидентов или инцидентов с серьёзными последствиями.

Дополнительная информация

Оценка инцидентов нарушения информационной безопасности может указывать на необходимость в совершенствовании существующих или внедрении дополнительных мероприятий по управлению информационной безопасностью с целью сведения к минимуму вероятности появления инцидентов нарушения информационной безопасности, снижения

возможного ущерба и расходы в будущем, кроме того, данную информацию следует учитывать при пересмотре политики информационной безопасности (5.1.2).

13.2.3 Сбор доказательств

Определение

Там, где дополнительное расследование против лица или организации после нарушения информационной безопасности включает судебное разбирательство (гражданское или уголовное), доказательства должны быть собраны, сохранены и в случае чего предъявлены, а также должны соответствовать правовым нормам свидетельствования, изложенным в соответствующем законодательстве.

Руководство по реализации

Необходимо разработать и соблюдать внутренние процедуры в целях наложения дисциплинарного взыскания внутри организации при сборе и предъявления доказательств.

В общем, правовые нормы сбора доказательств включают:

a) допустимость свидетельств: действительно ли свидетельства могут использоваться в суде или нет;

b) весомость свидетельств: качество и полнота свидетельств.

Чтобы достичь признания допустимости свидетельств, организациям необходимо обеспечить уверенность в том, что их информационные системы соответствуют всем юридическим требованиям и правилам в отношении допустимых свидетельств.

Весомость предоставленных доказательств должна соответствовать любым применяемым требованиям. Для получения весомости доказательств, качество и завершённость мер защиты, используемых для должной и последовательной защиты доказательств (т.е. доказательство контроля за процессом) в течении всего периода хранения и обработки доказательства, предназначенного для восстановления, должно быть представлено убедительное подтверждение свидетельств. В общем случае, такие убедительные подтверждения быть достигнуты следующим образом:

a) для бумажных документов: оригинал хранится безопасным способом, и фиксируется, кто нашел его, где он был найден, когда он был найден и кто засвидетельствовал обнаружение. Необходимо, чтобы любое исследование подтвердило, что оригиналы никто не пытался исказить;

b) для информации на компьютерных носителях: зеркальные изображения или копии (в зависимости от применяемых требований) любых сменных носителей, информации на жестких дисках или основной памяти компьютера следует выполнять таким образом, чтобы обеспечивать доступность. Журнал всех действий, выполненных в течение процесса копирования, необходимо сохранять, а сам процесс копирования необходимо засвидетельствовать. Одну копию носителей информации и журнал (если это невозможно, то, по крайней мере, одно зеркальное отражение или копию) следует хранить безопасным и неприкосновенным способом.

Любая судебная экспертиза должна проводиться только на копиях доказательственного материала. Целостность всего доказательственного материала должна быть защищена. Копирование доказательственного материала должно осуществляться под наблюдением доверенного персонала и информация о том, когда и где проводился процесс копирования, кто осуществлял копирование, какое оборудование и какие программы были задействованы, должно регистрироваться.

Дополнительная информация

Когда инцидент нарушения информационной безопасности обнаруживается впервые, не очевидно, что он может привести к возможным судебным разбирательствам. По-

этому, существует опасность, что необходимое показание будет случайно разрушено прежде, чем осознана серьезность инцидента. Целесообразно на самом раннем этапе привлекать юриста или полицию в любом случае предполагаемых судебных разбирательств, и получить консультацию относительно требуемых свидетельств.

Доказательства могут выходить за пределы организации и/или юрисдикционные границы. В таких случаях необходимо обеспечить, чтобы организация была правомочна собирать требуемую информацию как доказательства. Необходимо также учитывать требования различных судебных округов, чтобы увеличить до максимума шансы допуска на территориях соответствующих судебных округов.

14 Управление непрерывностью бизнеса

14.1 Аспекты информационной безопасности управления непрерывностью бизнеса

Цель: противодействие прерываниям бизнеса и защита критических бизнес-процессов от последствий значительных сбоев или бедствий и гарантия их своевременного возобновления.

Необходимо внедрить процесс управления непрерывностью бизнеса с целью минимизации влияния на организацию и восстановления после потери информационных активов (которые могут быть результатом природных бедствий, несчастных случаев, отказов оборудования, и преднамеренных действий) до приемлемого уровня с помощью комбинирования профилактических и восстановительных мероприятий по управлению информационной безопасностью. Этот процесс должен идентифицировать важные бизнес-процессы и интегрировать требования непрерывности бизнеса управления информационной безопасностью с другими требованиями непрерывности касательно таких аспектов, как операции, кадровое обеспечение, материалы, транспорт и оборудование.

Последствия бедствий, нарушений безопасности, отказов в обслуживании и доступность сервисов должны быть предметом анализа влияния на бизнес. Необходимо разрабатывать и внедрять планы обеспечения непрерывности бизнеса с целью возобновления важных операций в течение требуемого времени при их нарушении. Информационная безопасность должна быть составной частью общего процесса непрерывности бизнеса, и других процессов управления в организации.

Необходимо, чтобы управление непрерывностью бизнеса включало мероприятия по управлению информационной безопасностью для идентификации и уменьшения рисков, в дополнение к общему процессу оценки степени риска, ограничения последствий разрушительных инцидентов, и обеспечения доступности информации, требуемой для процессов бизнеса.

14.1.1 Включение информационной безопасности в процесс управления непрерывностью бизнеса

Определение

Необходимо разработать и поддерживать управляемый процесс непрерывности бизнеса для всей организации, который соответствует требованиям информационной безопасности, необходимым для обеспечения непрерывности бизнеса.

Руководство по реализации

В процессе должны быть собраны вместе следующие ключевые элементы управления непрерывности бизнеса:

а) понимание рисков, с которыми сталкивается организация, с точки зрения вероятности возникновения и последствий, включая идентификацию и определение

приоритетов критических бизнес-процессов (см. 14.1.2);

b) определение всех активов, задействованных в критических бизнес-процессах (см. 7.1.1);

c) понимание возможных последствий нарушения бизнес-процессов, вызванных инцидентами нарушения информационной безопасности, в случае незначительных или существенных инцидентов, потенциально угрожающих жизнедеятельности организации, а также выбора средств и способов обработки информации соответствующих к целям бизнеса;

d) организация оптимального страхования результатов обработки информации, которое может быть частью общего процесса непрерывности бизнеса, а также частью управления операционным риском;

e) определение и рассмотрение вопроса реализации дополнительных превентивных и подавляющих средств контроля;

f) идентификация достаточных финансовых, организационных, технических ресурсов и ресурсов окружающей среды для соответствия идентифицированным требованиям информационной безопасности;

g) обеспечение безопасности персонала и защиты средств обработки информации и собственности организации;

h) формулирование и документирование планов обеспечения непрерывности бизнеса, удовлетворяющих требования информационной безопасности в соответствии с согласованной стратегией (см. 14.1.3);

i) регулярное тестирование и обновление планов развития информационных технологий и существующих процессов (см. 14.1.5);

j) обеспечение органичного включения в процессы и структуру организации планов управления непрерывностью бизнеса. Ответственность за координацию процесса управления непрерывностью бизнеса следует возлагать на орган, обладающий соответствующими полномочиями в организации, например, на управляющий совет по информационной безопасности (см. 6.1.1).

14.1.2 Непрерывность бизнеса и оценка риска

Определение

Случаи, которые могут вызывать прерывания в бизнес-процессах, должны быть идентифицированы наряду с вероятностью и степенью воздействия таких прерываний и их последствия для информационной безопасности.

Руководство по реализации

Аспекты информационной безопасности непрерывности бизнеса должны основываться на идентификации случаев (или последовательности случаев), которые могут привести к прерываниям в бизнес-процессах организаций, например, отказ оборудования, ошибки оператора, воровство, пожар, стихийные бедствия и террористические акты. После них должна проводиться оценка рисков для определения вероятности и воздействия таких прерываний с точки зрения времени, масштабов ущерба и периода восстановления.

Оценки рисков для непрерывности бизнеса должны проводиться при участии владельцев бизнес-ресурсов и процессов. Эта оценка должна учитывать все бизнес-процессы и не должна ограничиваться средствами обработки информации, но должна включать результаты специфические для информационной безопасности. Важно связать вместе различные аспекты риска, чтобы получить полное представление о требованиях непрерывности бизнеса организации. При оценке необходимо идентифицировать, определять количество и приоритеты рисков в сравнении с критериями и целями организации, включая критические ресурсы, воздействия прерывания, допустимое время простоя и приоритеты восстановления.

В зависимости от результатов оценки рисков, необходимо разработать стратегию для определения общего подхода к обеспечению непрерывности бизнеса. Разработанная стратегия должна быть утверждена руководством организации и согласована с планом.

14.1.3 Разработка и реализация планов обеспечения непрерывности бизнеса, включая информационную безопасность

Определение

Следует разрабатывать и реализовывать планы по поддержке или восстановлению операций и гарантировать доступность информации на требуемом уровне в требуемые периоды времени после прерывания или отказа критических бизнес-процессов.

Руководство по реализации

Необходимо, чтобы план обеспечения непрерывности бизнеса предусматривал следующие мероприятия по обеспечению информационной безопасности:

a) определение и согласование всех обязанностей должностных лиц и процедур по обеспечению непрерывности бизнеса;
b) идентификацию приемлемых потерь информации и услуг;
c) внедрение в случае чрезвычайных ситуаций процедур обеспечивающих возможность восстановления бизнес-процессов и доступности информации в течение требуемого времени. Особое внимание следует уделять оценке зависимости бизнеса от внешних и внутренних факторов и существующих контрактов;
d) операционные процедуры, следующие за завершением восстановления и возобновления;
e) документирование согласованных процедур и процессов;
f) соответствующее обучение сотрудников действиям в случаях чрезвычайных ситуаций, включая кризисное управление;
g) тестирование и обновление планов обеспечения непрерывности бизнеса.

Необходимо, чтобы план обеспечения непрерывности бизнеса соответствовал требуемым целям бизнеса, например, в отношении восстановления определенных сервисов для клиентов в приемлемый промежуток времени. Сервисы и ресурсы должны идентифицироваться, включая укомплектование персоналом, альтернативные ресурсы средств обработки информации, а также меры по переходу на аварийный режим работы для средств обработки информации. Такие меры по переходу на аварийный режим могут включать договорённости с третьими сторонами в виде соглашений, основанных на взаимности, или услуг коммерческой подписки.

Планы обеспечения непрерывности бизнеса должны учитывать уязвимости организации, и, следовательно, могут содержать секретную информацию, которая должна быть должным образом защищена. Копии планов должны храниться в удалённом месте, чтобы избежать повреждения в случае бедствия в главном здании. Руководство должно обеспечивать постоянное обновление копий планов обеспечения непрерывности бизнеса и их защиту на том же уровне безопасности, который применяется в главном здании. Остальной материал, необходимый для выполнения планов обеспечения непрерывности бизнеса также должен храниться в удалённом месте.

В случае использования для хранения временных помещений уровень задействованных средств контроля безопасности в этих помещениях должен быть эквивалентным уровню в главном помещении.

Дополнительная информация

Необходимо отметить, что планы и действия по управлению кризисными ситуациями (см.14.1.3f) могут отличаться от управления непрерывностью бизнеса, т.е. может возникнуть кризисная ситуация, которая может быть разрешена обычными процессами

управления.

14.1.4 Структура планов обеспечения непрерывности бизнеса

Определение

Следует поддерживать единую структуру планов обеспечения непрерывности бизнеса, для обеспечения непротиворечивости всех планов и удовлетворения всех планов, и определить приоритеты для тестирования и обслуживания средств и систем обработки информации.

Руководство по реализации

В каждом плане обеспечения непрерывности бизнеса должен описываться метод обеспечения непрерывности, например, метод обеспечения доступности и безопасности информации или информационной системы. Каждый план должен также обозначать план эскалации (расширения) и условия его реализации, а также должностных лиц, ответственных за выполнения каждого пункта плана. Когда идентифицируются новые требования, любые существующие процедуры чрезвычайных ситуаций, например, планы по эвакуации или меры по переходу на аварийный режим, должны соответствующим образом корректироваться. Для обеспечения решения проблем обеспечения непрерывности бизнеса должным образом в программу управления внесением изменений организации должны быть включены отдельные процедуры.

Необходимо, чтобы за каждый план отвечал конкретный руководитель (сотрудник). Чрезвычайные меры, планы по переходу на аварийный режим ручной обработки, планы по возобновлению следует включать в сферу ответственности владельцев соответствующих бизнес-ресурсов или участников затрагиваемых процессов. За меры по переходу на аварийный режим работы с использованием альтернативных технических сервисов, таких как средства обработки информации и средства связи, ответственность обычно несут поставщики услуг.

Необходимо, чтобы структура планов обеспечения непрерывности бизнеса удовлетворяла идентифицированные требования информационной безопасности и предусматривалось следующее:

a) условия реализации планов, которые определяют порядок действий должностных лиц, которому необходимо следовать (например, как оценивать ситуацию, кто должен принимать участие, и т. д.), перед введением в действие каждого плана;
b) процедуры на случай чрезвычайных ситуаций, которые должны быть предприняты после инцидента, подвергающего опасности бизнес операции;
c) процедуры перехода на аварийный режим работы, которые описывают необходимые действия по переносу важных бизнес-операций или сервисов поддержки в альтернативное временное место размещения и восстановлению бизнес-процессов в требуемые периоды времени;
d) временные операционные процедуры, следующие за завершением восстановления и возобновления;
e) процедуры возобновления, которые описывают необходимые действия, для возвращения к нормальному режиму ведения бизнеса;
f) график поддержки плана, который определяет сроки и методы тестирования, а также описание процесса поддержки плана;
g) мероприятия по обучению персонала, которые направлены на понимание процессов обеспечения непрерывности бизнеса сотрудниками, и поддержание постоянной эффективности этих процессов;
h) обязанности должностных лиц, ответственных за выполнение каждого пункта плана. При необходимости должны быть указаны альтернативные ответствен-

ные;

i) критические активы и ресурсы, необходимы для выполнения аварийных процедур, процедур перехода в аварийный режим и процедур возобновления.

14.1.5 Тестирование, поддержание и пересмотр планов обеспечения непрерывности бизнеса

Определение

Планы обеспечения непрерывности бизнеса должны постоянно тестироваться и обновляться, чтобы быть эффективными и отвечать новейшим требованиям.

Руководство по реализации

Тесты плана непрерывности бизнеса необходимы для обеспечения знания своих обязанностей по непрерывности бизнеса и безопасности информации всеми членами команды восстановления и другим персоналом, имеющим к этому отношение.

Необходимо, чтобы в графике тестирования плана(ов) по обеспечению непрерывности бизнеса указывалось, как и когда следует проверять каждый пункт плана. Каждый элемент плана (ов) должны периодически тестироваться.

Методы тестирования могут быть различными. При этом могут использоваться следующие методы:

a) тестирование ("имитация прогона") различных сценариев (обсуждение мер по восстановлению бизнеса на различных примерах прерываний);
b) моделирование (особенно для тренировки персонала по выполнению своих функций после инцидента и переходе к кризисному управлению);
c) тестирование технического восстановления (обеспечение уверенности в эффективном восстановлении информационных систем);
d) проверку восстановления в альтернативном месте (бизнес-процессы осуществляются параллельно с операциями по восстановлению в удаленном альтернативном месте);
e) тестирование средств и сервисов поставщиков (обеспечение уверенности в том, что предоставленные сторонними организациями сервисы и программные продукты удовлетворяют контрактным обязательствам);
f) "генеральные репетиции" (тестирование того, что организация, персонал, оборудование, средства и процессы могут справляться с прерываниями).

Методы тестирования могут использоваться любой организацией. Они должны применяться способом релевантным плану восстановления. Результаты тестирований должны записываться и предпринятые действия, должны улучшать планы.

Необходимо назначать ответственных за проведение регулярных пересмотров плана по обеспечению непрерывности бизнеса; идентифицированные изменения в бизнес-процессах, еще не отраженные в планах по обеспечению непрерывности бизнеса, должны быть учтены путем соответствующих обновлений планов. Формализованный процесс управления изменениями должен обеспечивать рассылку и ввод в действие обновленных планов в рамках их регулярных пересмотров.

Примерами изменений, которые должны учитываться при обновлении планов обеспечения непрерывности бизнеса, являются изменения, вносимые при приобретении нового оборудования, модернизации систем, и изменения, связанные с:

a) персоналом;
b) адресами или номерами телефонов;
c) стратегией бизнеса;
d) местоположением, средствами и ресурсами;
e) законодательством;
f) подрядчиками, поставщиками и основными клиентами;

g) процессами (как новыми, так и изъятыми);
h) рисками (операционными и финансовыми).

15 Соответствие требованиям

15.1 Соответствие правовым требованиям

Цель: предотвращение любых нарушений норм уголовного и гражданского права, обязательных предписаний и регулирующих требований или договорных обязательств, а также требований безопасности.

Проектирование и функционирование информационных систем, их использование и управление ими могут быть предметом обязательных предписаний, регулирующих требований, а также требований безопасности в договорных обязательствах.

Следует консультироваться с юристами организации или с практикующими юристами, имеющими соответствующую квалификацию, в отношении конкретных юридических вопросов. Следует иметь в виду, что законодательные требования в отношении информации, созданной в одной стране и переданной в другую страну (например, информационный поток, передаваемый за границу государства) различаются в разных странах.

15.1.1 Идентификация пригодного законодательства

Определение

Все применяемые нормы законодательства, обязательные предписания, регулирующие требования и договорные обязательства и подход организации к удовлетворению этих требований следует четко определять, документировать и придерживаться для каждой информационной системы и организации.

Руководство по реализации

Конкретные мероприятий по обеспечению информационной безопасности и индивидуальные обязанности должностных лиц по выполнению этих требований необходимо определять и документировать соответствующим образом.

15.1.2 Права на интеллектуальную собственность (IPR)

Определение

Для обеспечения соответствия правовым, обязательным и договорным требованиям по использованию материала, для которого могут существовать права на интеллектуальную собственность, и по использованию продукции частного программного обеспечения необходимо внедрить соответствующие процедуры.

Руководство по реализации

Для защиты любого материала, который может считаться интеллектуальной собственностью, следует рассмотреть следующие правила:

a) строгое следование требованиям авторского права, которое определяет законное использование программных и информационных продуктов;
b) приобретение программного обеспечения только у известных и имеющих хорошую репутацию источников, чтобы не было нарушено авторское право;
c) обеспечение осведомленности сотрудников по вопросам политик защиты авторского права, а также уведомление о применении дисциплинарных санкций к нарушителям;
d) ведение соответствующих регистров активов, и идентификация всех активов с требованиями к защите прав на интеллектуальную собственность;
e) ведение подтверждений и доказательств собственности на лицензии, дистрибутивные диски, руководства, и т.д.;

f) контроль за соблюдением ограничений максимального числа разрешенных пользователей программными продуктами;
g) регулярные проверки применения только авторизованного программного обеспечения и лицензированных продуктов;
h) реализация политики по обеспечению выполнения условий соответствующих лицензионных соглашений;
i) выполнение правил утилизации или передачи программного обеспечения на сторону;
j) организация регулярного аудита;
k) соблюдение условий получения из общедоступных сетей программного обеспечения и информации;
l) недублирование, преобразование в другой формат или удаление из коммерческих записей (плёнка, аудио) иначе, чем предусмотрено авторским правом;
m) некопирование, полностью или частично, книг, статей, докладов или других документов, кроме тех, что разрешены авторским правом.

Дополнительная информация

Права на интеллектуальную собственность включают авторское право на программное обеспечение или документ, право на конструкцию, торговые марки, патенты и лицензии исходных кодов.

Программные продукты, являющиеся предметом чьей-то собственности, обычно поставляются в рамках лицензионного соглашения, которое определяет условия лицензирования, ограничивает использование продуктов определенными компьютерами, а также может ограничивать копирование их только с целью создания резервных копий. Ситуация с правами на интеллектуальную собственность в виде программного обеспечения, разработанного организацией, требует разъяснения среди персонала.

Законодательные, регулирующие и договорные требования могут вводить ограничения на копирование материалов, являющихся предметом собственности. В частности, эти ограничения могут содержать требования к использованию только тех материалов, которые или разработаны организацией, или лицензированы, или предоставляются разработчиком для организации. Нарушение авторских прав может привести к инициированию судебного процесса, который может включать уголовное преследование.

15.1.3 Защита учётных записей организации

Определение

Важные данные необходимо защищать от утраты, разрушения и фальсификации в соответствии с законодательными, регулирующими и договорными требованиями.

Руководство по реализации

Данные необходимо классифицировать по типам, например, бухгалтерские записи, записи баз данных, журналы транзакций, журналы аудита и операционных процедур, каждый с указанием периодов хранения и типов носителей хранимых данных (бумага, микрофильм, магнитные или оптические носители). Любые криптографические ключи, связанные с зашифрованными архивами или цифровыми подписями (см. 12.3), должны храниться для инициирования дешифровки записей на период времени хранения записей.

Следует учитывать возможность снижения качества носителей, используемых для хранения данных, осуществлять процедуры по хранению и уходу за носителями данных в соответствии с рекомендациями изготовителя. Следует рассматривать использование бумаги и диамикрокарты длительное время.

При использовании электронных носителей данных, следует применять процедуры проверки возможности доступа к данным (читаемость, как самих носителей, так и формата данных) в течение периода хранения, с целью защиты от потери вследствие будущих изменений технологии.

Системы хранения данных следует выбирать таким образом, чтобы требуемые данные могли быть извлечены приемлемым способом, в зависимости от требований, которые нужно выполнить.

Необходимо, чтобы система хранения обеспечивала четкую идентификацию данных, а также их периода хранения, установленного национальным или региональным законом или регулирующими требованиями. Необходимо, чтобы эта система предоставляла возможности по уничтожению данных после того периода, когда у организации отпадет потребность в их хранении.

С целью выполнения данных обязательств, организации следует:

a) разработать руководство в отношении сроков, порядка хранения и утилизации информации;
b) составить график хранения наиболее важных данных;
c) вести опись источников ключевой информации;
d) внедрить соответствующие меры для защиты информации от потери, разрушения и фальсификации.

Дополнительная информация

В отношении некоторых данных может потребоваться обеспечение безопасности хранения с целью выполнения законодательных или регулирующих требований, а также поддержки важных бизнес-приложений. В качестве примеров можно привести данные, которые могут потребоваться для доказательства того, что организация работает в рамках установленных законом норм или регулирующих требований, с целью адекватной защиты от потенциального гражданского или уголовного преследования, а также подтверждения финансового состояния организации для акционеров, партнеров и аудиторов. Период времени хранения и содержание данных может быть установлен в соответствии с государственным законом или регулирующими требованиями.

Дальнейшую информацию об управлении данными организации можно найти в [18].

15.1.4 Защита данных и неприкосновенность персональной информации

Определение

Защита данных и неприкосновенность личной жизни должны гарантироваться, как это предусмотрено в релевантном законодательстве, положениях и, если это приемлемо, в условиях договора.

Руководство по реализации

Необходимо разработать политику защиты данных и неприкосновенности личной жизни. Эта политика должна быть известна всем лицам, участвующим в обработке персональной информации.

Соответствие политике и законодательству по защите данных требует соответствующей структуры управления информационной безопасностью. Лучше всего это достигается при назначении должностного лица отвечающего за защиту данных, обеспечивающего соответствующие разъяснения менеджерам, пользователями и поставщиками услуг об их индивидуальной ответственности, а также контролирующего выполнение соответствующих мероприятий по обеспечению информационной безопасности. Ответственность за обработку персональной информации и обеспечение осведомлённости о принципах защиты данных должна рассматриваться с точки зрения соответствия релевантному законодательству и правовым нормам. Необходимо реализовать соответствующие технические и организационные меры по защите персональной информации.

Дополнительная информация

В ряде стран введены нормы законодательства, в которых установлены ограничения в отношении обработки и передачи персональных данных (в основном, это касается информации о живущих людях, которые могут быть идентифицированы по этой информа-

ции). В зависимости от национального законодательства, такие ограничения могут налагать обязанности на тех, кто осуществляет сбор, обработку и распространение личной информации, а также могут ограничивать возможность передачи этих данных в другие страны.

15.1.5 Предотвращение злоупотребления средствами обработки информации

Определение

Необходимо удерживать пользователей от применения средств обработки информации в несанкционированных целях.

Руководство по реализации

Руководство должно одобрить использование средств обработки информации.

Любое использование этих средств для непроизводственных или неавторизованных целей, без одобрения руководства (см. 6.1.4), следует расценивать как нецелевое. Если такая несанкционированная деятельность выявлена мониторингом или другими способами, то на это следует обратить внимание непосредственного руководителя сотрудника, для принятия соответствующих мер дисциплинарного и/или юридического воздействия.

Перед реализацией процедур мониторинга необходима консультация юриста.

Все пользователи должны быть осведомлены о четких рамках разрешенного им доступа и о мониторинге по обнаружению несанкционированного использования. Это может быть достигнуто путем ознакомления пользователей под роспись с предоставленной им авторизацией в письменной форме, а организации следует безопасным способом сохранять копию этого документа. Необходимо, чтобы сотрудники организации, подрядчики и пользователи третьей стороны были осведомлены о том, что во всех случаях они имеют право доступа только к тем данным, пользование которыми им разрешено.

Необходимо, чтобы при регистрации доступа к системе на экране компьютера было отражено предупреждающее сообщение, указывающее, что система, вход в которую пользователи пытаются осуществить, является системой с ограниченным доступом, и что несанкционированный доступ к ней запрещен. Пользователь должен подтвердить прочтение и реагировать соответствующим образом на это сообщение, чтобы продолжить процесс регистрации (см. 11.5.1).

Дополнительная информация

Средства обработки информации предназначены в первую очередь или исключительно для целей деловой деятельности.

Обнаружение вторжения, проверка содержания и другие средства мониторинга могут содействовать в предотвращении и обнаружении злоупотребления средствами обработки информации.

Многие страны имеют законодательство по защите от неправильного использования компьютеров. Возможны случаи использования компьютера для неавторизованных целей с преступным умыслом.

Законность использования мониторинга зависит от действующего в стране законодательства и может потребоваться, чтобы сотрудники были осведомлены и/или дали документированное согласие на проведение мониторинга. Там, где система, в которую осуществляется вход, используется для общественного доступа (например, общественный web-сервер) и является предметом мониторинга безопасности, должно отображаться информирующее об этом сообщение.

15.1.6 Регулирование использования средств криптографии

Определение

Средства криптографии должны применяться в соответствии со всеми релевантными соглашениями, законами и правовыми нормами.

Руководство по реализации

Последующие пункты необходимо рассмотреть на соответствие действующим законам, соглашениям и правовым нормам:

a) ограничения импорта и/или экспорта аппаратных и программных средств для выполнения криптографических функций;
b) ограничения импорта и/или экспорта аппаратных и программных средств, которые разработаны таким образом, что имеют, как дополнение, криптографические функции;
c) ограничения на использование шифрования;
d) обязательные или дискреционные методы доступа со стороны государства к информации, зашифрованной с помощью аппаратных или программных средств для обеспечения конфиденциальности содержания;

Для обеспечения уверенности в соответствии политики использования криптографических средств в организации национальному законодательству и положениям, необходима консультация юриста. Прежде, чем зашифрованная информация или криптографическое средство будут переданы в другую страну, необходимо также получить консультацию юриста.

15.2 Соответствие политикам и стандартам безопасности, и техническое соответствие

Цель: обеспечивать соответствие систем политике безопасности организации и стандартам.

Безопасность информационных систем необходимо регулярно анализировать (пересматривать).

Такие анализы (пересмотры) необходимо осуществлять относительно соответствующих политик безопасности, а технические платформы и информационные системы должны подвергаться аудиту не предмет соответствия стандартам внедрения средств безопасности и документированным мерам контроля безопасности.

15.2.1 Соответствие политикам и стандартам безопасности

Определение

Руководители должны обеспечить правильное выполнение всех процедур безопасности в пределах их сферы ответственности для достижения соответствия с политиками и стандартами безопасности.

Руководство по реализации

Руководители должны регулярно пересматривать соответствие обработки информации в их сфере ответственности с соответствующими политиками и стандартами безопасности, а также с любыми другими требованиями безопасности.

Если в результате этого пересмотра обнаружено какое-либо несоответствие, руководители должны:

a) определить причины несоответствия;
b) оценить необходимость действий для того, чтобы это несоответствие больше не возникало;
c) определить и реализовать соответствующие коррективные меры;
d) пересмотреть уже предпринятые коррективные меры.

Результаты пересмотров и коррективных действий, проведённых руководителями, должны регистрироваться, а регистрационные записи сохраняться. Руководители должны информировать лиц, проводящих независимые пересмотры (см. 6.1.8) о результатах, когда независимый пересмотр происходит в сфере их ответственности.

Дополнительная информация

Оперативный мониторинг системы приводится в пункте 10.10

15.2.2 Проверка технического соответствия

Определение

Информационные системы следует регулярно проверять на соответствие стандартам обеспечения безопасности.

Руководство по реализации

Проверка технического соответствия может выполняться вручную (если необходимо, с помощью инструментальных программных средств) опытным специалистом по системам и/или с помощью автоматизированных программных средств, которые выдают технический отчёт для последующего интерпретирования техническим специалистом.

При применении испытаний на проникновение или оценок уязвимости необходимо соблюдать осторожность, поскольку такие действия могут привести к созданию опасности для безопасности системы. Подобные испытания должны планироваться, документироваться и быть воспроизводимыми.

Любую проверку технического соответствия следует выполнять только компетентным, авторизованным лицам, либо под их наблюдением.

Дополнительная информация

Проверка технического соответствия включает проверку операционных систем, чтобы убедиться в правильности реализации средств контроля программного и аппаратного обеспечения. Для этого типа проверки соответствия требуется техническая экспертиза специалиста.

Проверка соответствия также охватывает, например, тестирование на проникновение и оценки уязвимостей, которые могут быть выполнены независимыми экспертами, специально приглашенными по контракту для этого. Данное тестирование может быть полезным для обнаружения уязвимостей в системе и для проверки того, насколько эффективны средства контроля при предотвращении несанкционированного доступа вследствие этих уязвимостей.

Испытание на проникновение и оценки уязвимости обеспечивают «мгновенный снимок» системы в определённом состоянии в определённое время. «Мгновенный снимок» ограничивается частями системы, испытываемыми во время попытки проникновения. Испытание на проникновение и оценки уязвимости не подменяют оценки риска.

15.3 Вопросы для рассмотрения при аудите информационных систем

Цель: максимизировать эффективность и минимизировать влияние, связанное с процессом аудита системы.

Необходимо иметь средства контроля для обеспечения безопасности систем операционной среды и инструментальных средств аудита в процессе аудита систем.

Защита также требуется для защиты целостности и предотвращения неправильного использования инструментальных средств аудита.

15.3.1 Средства контроля аудита информационных систем

Определение

Требования и действия аудита, включающие проверки систем операционной среды, необходимо тщательно планировать и согласовывать, чтобы сводить к минимуму риск для бизнес-процессов.

Руководство по реализации

Необходимо соблюдать следующие правила:

a) требования аудита необходимо согласовать с соответствующим руководством;
b) объем работ по проверкам следует согласовывать и контролировать;
c) при проведении проверок необходимо использовать доступ только для чтения к программному обеспечению и данным;
d) другие виды доступа, кроме доступа только для чтения, может быть разрешен только в отношении изолированных копий файлов системы, которые необходимо удалять по завершению аудита, или соответствующим образом защищать, если существует обязанность хранения подобных файлов по требованиям документации аудита;
e) необходимо четко идентифицировать и обеспечить доступность ресурсов, необходимых для выполнения проверок;
f) требования в отношении специальной или дополнительной обработки данных следует идентифицировать и согласовывать;
g) весь доступ должен подвергаться мониторингу и регистрироваться с целью обеспечения протоколирования для последующих ссылок; для критических данных или систем нужно рассматривать использование последующих ссылок с отметкой времени;
h) все процедуры, требования и обязанности следует документировать;
i) лицо, проводящее аудит, должно быть независимым от ревизируемых действий.

15.3.2 Защита инструментальных средств аудита информационных систем

Определение

Доступ к средствам аудита информационных систем необходимо защищать, чтобы предотвращать любое возможное их неправильное использование или компрометацию.

Руководство по реализации

Инструментальные средства аудита информационных систем, например, программное обеспечение или файлы данных, должны быть отделены от систем разработки и операционных систем и не должны находиться в библиотеках на лентах или в зоне пользователя, если им не будет придан соответствующий уровень защиты.

Дополнительная информация

Если в аудите участвуют третьи стороны, может существовать риск злоупотребления инструментальными средствами аудита этими третьими сторонами, и информацией, к которой имеет доступ организация третьей стороны. Для устранения этого риска можно рассмотреть такие средства, как 6.2.1 (оценка рисков) и 9.1.2 (ограничение физического доступа) и необходимо учесть такие последствия, как немедленная смена паролей, раскрытых аудиторам.

Приложение
(справочное)

Библиография

[1] Руководящие указания	Руководящие указания OECD по обеспечению безопасности информационных систем и сетей: «Навстречу культуре безопасности», 2002г. OECD Guidelines for the Security of Information Systems and Networks: 'Towards a Culture of Security', 2002.
[2] ISO/IEC 13335-1:2004[1]	Технологии информационные. Методы защиты. Управление защитой информационно-коммуникационных технологий. Часть 1. Концепции и модели управления защитой информационно-коммуникационных технологий (Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management)
[3] ISO/IEC TR 18044[1]	Технологии информационные. Методы защиты. Управление нарушениями безопасности информации (Information technology – Security techniques – Information security incident management)
[4] ISO/IEC Guide 73:2002[1]	Risk management – Vocabulary – Guidelines for use in standards
[5] ISO/IEC Guide 2:1996[1]	Standardization and related activities – General vocabulary
[6] ISO/IEC TR 13335-3:1998[1]	Информационная технология. Руководящие указания по контролю безопасности информационных технологий. Часть 3. Методы контроля IT (Information technology – Guidelines for the Management of IT Security – Part 3: Techniques for the management of IT Security)
[7] ISO 19011:2002[2]	Guidelines for quality and /or environmental management systems auditing
[8] ISO/IEC 18028-4[1]	Технологии информационные. Методы обеспечения защиты. Защита сетевых технологий (IT). Часть 4. Защищенный дистанционный доступ (Information technology – Security techniques – IT Network security – Part 4: Securing remote access)
[9] ISO/IEC 15408-1:1999[2]	Information technology – Security techniques – Evaluation Criteria for IT security – Part 1: Introduction and general model
[10] IEEE P1363-2000[1]	Standard Specifications for Public-Key Cryptography
[11] Руководящие указания	Руководящие указания OECD в отношении политики криптографии, 1997г. OECD Guidelines for Cryptography Policy, 1997.

[1] Использование международных стандартов возможно в соответствии с СТ РК 1.9 За приобретением данных стандартов можно обращаться в государственный фонд нормативно-правовых актов и стандартов по адресу: г.Астана, Левый берег р.Ишим, ул.№ 35, дом 11 здание «Эталонный центр».

[2] При применении настоящих стандартов рекомендуется использовать вместо ссылочных международных стандартов соответствующие им государственные стандарты, сведения о которых приведены в дополнительном приложении.

[12] ISO/IEC 11770-1:1996[1] Информационная технология. Методика обеспечения защиты данных. Ключевое управление. Часть 1. Структуры (Information technology – Security techniques – Key management – Part 1:Framework)

[13] ISO/IEC 9796-2:2002[1] Информационные технологии. Методы обеспечения безопасности. Схемы цифровой подписи, позволяющие восстанавливать сообщения. Часть 2. Механизмы, основанные на факторизации целого числа (Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms)

[14] ISO/IEC 9796-3:2000[1] Информационные технологии. Методы защиты. Схемы цифровой сигнатуры, позволяющие восстанавливать сообщения. Часть 3. Механизмы, основанные на дискретном логарифме (Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms)

[15] ISO/IEC 14888-1:1998[2] Information technology – Security techniques – Digital signatures with appendix – Part 1: General

[16] ISO 10007:2003[1] Quality management systems – Guidelines for configuration management

[17] ISO/IEC 12207:1995[1] Информационные технологии. Процессы жизненного цикла программного обеспечения (Information technology – Software life cycle processes)

[18] ISO 15489-1:2001[1] Information and documentation – Records management – Part 1: General

[1] Использование международных стандартов возможно в соответствии с СТ РК 1.9 За приобретением данных стандартов можно обращаться в государственный фонд нормативно-правовых актов и стандартов по адресу: г.Астана, Левый берег р.Ишим, ул.№ 35, дом 11 здание «Эталонный центр».

[2] При применении настоящих стандартов рекомендуется использовать вместо ссылочных международных стандартов соответствующие им государственные стандарты, сведения о которых приведены в дополнительном приложении.

Приложение
(справочное)

Сведения о соответствии ссылочного международного стандарта государственному стандарту

Обозначение ссылочного стандарта	Обозначение и наименование соответствующего государственного стандарта
ISO 19011:2002	СТ РК ИСО 19011-2002 Рекомендации по аудиту систем менеджмента качества и/или охраны окружающей среды.
ISO/IEC 15408-1:1999	СТ РК ГОСТ Р ИСО/МЭК 15408-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»
ISO/IEC 14888-1:1998	СТ РК ИСО/МЭК 14888–1-2006 «Информационная технология. Методы защиты информации. Цифровые подписи с приложением. Часть 1. Общие положения»

УДК **МКС 35.040**
01.040.01

Ключевые слова: информационная технология, информационная безопасность, риски, активы, охраняемая зона, контроль доступа, аудит, документально оформленная процедура, инцидент информационной безопасности

Басуға _____ж. қол қойылды Пішімі 60х84 1/16
Қағазы офсеттік. Қаріп түрі «KZ Times New Roman»,
«Times New Roman»
Шартты баспа табағы 1,86. Таралымы ____ дана. Тапсырыс ____

«Қазақстан стандарттау және сертификаттау институты»
республикалық мемлекеттік кәсіпорны
010000, Астана қаласы, Есіл өзенінің жағалауы, № 35 көше, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 240074