ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27002— 2012

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Свод норм и правил менеджмента информационной безопасности

ISO/IEC 27002:2005
Information technology — Security techniques — Code of practice for information security management
(IDT)

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (ООО «НПФ «Кристалл») и Обществом с ограниченной ответственностью «Информационный аналитический вычислительный центр» (ООО «ИАВЦ») на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 24 сентября 2012 г. № 423-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27002:2005 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» (ISO/IEC 27002:2005 «Information technology — Security techniques — Code of practice for information security management»).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5 (пункт 3.5).

5 ВЗАМЕН ГОСТ Р ИСО/МЭК 17799—2005

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru)

© Стандартинформ, 2014

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

Содержание

1 Область применения . . . 1
2 Термины и определения . . . 1
3 Структура настоящего стандарта . . . 3
3.1 Разделы . . . 3
3.2 Основные категории безопасности . . . 3
4 Оценка и обработка рисков . . . 3
4.1 Оценка рисков безопасности . . . 3
4.2 Обработка рисков безопасности . . . 4
5 Политика безопасности . . . 5
5.1 Политика информационной безопасности . . . 5
6 Организационные аспекты информационной безопасности . . . 6
6.1 Задачи, решаемые внутри организации . . . 6
6.2 Аспекты взаимодействия со сторонними организациями . . . 10
7 Менеджмент активов . . . 15
7.1 Ответственность за активы . . . 15
7.2 Классификация информации . . . 16
8 Безопасность, связанная с персоналом . . . 17
8.1 Перед трудоустройством . . . 17
8.2 В течение занятости . . . 19
8.3 Прекращение или смена занятости . . . 21
9 Физическая безопасность и защита от воздействий окружающей среды . . . 22
9.1 Зоны безопасности . . . 22
9.2 Безопасность оборудования . . . 25
10 Менеджмент коммуникаций и работ . . . 29
10.1 Эксплуатационные процедуры и обязанности . . . 29
10.2 Менеджмент оказания услуг третьей стороной . . . 31
10.3 Планирование и приемка систем . . . 32
10.4 Защита от вредоносной и мобильной программы . . . 33
10.5 Резервирование . . . 35
10.6 Менеджмент безопасности сети . . . 36
10.7 Обращение с носителями информации . . . 37
10.8 Обмен информацией . . . 39
10.9 Услуги электронной торговли . . . 42
10.10 Мониторинг . . . 44
11 Управление доступом . . . 47
11.1 Требование бизнеса по управлению доступом . . . 47
11.2 Менеджмент доступа пользователей . . . 48
11.3 Обязанности пользователя . . . 50
11.4 Управление доступом к сети . . . 52
11.5 Управление доступом к эксплуатируемой системе . . . 55
11.6 Управление доступом к информации и прикладным программам . . . 58
11.7 Мобильная вычислительная техника и дистанционная работа . . . 59
12 Приобретение, разработка и эксплуатация информационных систем . . . 61
12.1 Требования безопасности информационных систем . . . 61
12.2 Корректная обработка в прикладных программах . . . 62
12.3 Криптографические меры и средства контроля и управления . . . 64
12.4 Безопасность системных файлов . . . 66
12.5 Безопасность в процессах разработки и поддержки . . . 68
12.6 Менеджмент технических уязвимостей . . . 71
13 Менеджмент инцидентов информационной безопасности . . . 72
13.1 Оповещение о событиях и уязвимостях информационной безопасности . . . 72
13.2 Менеджмент инцидентов информационной безопасности и необходимое совершенствование 74

14 Менеджмент непрерывности бизнеса 76
14.1 Аспекты информационной безопасности в рамках менеджмента непрерывности бизнеса . . . 76
15 Соответствие 80
15.1 Соответствие требованиям законодательства 80
15.2 Соответствие политикам безопасности и стандартам, техническое соответствие 83
15.3 Рассмотрение аудита информационных систем 84
Библиография 86

0 Введение

0.1 Что такое информационная безопасность?

Информация — это актив, который, подобно другим активам организации, имеет ценность и, следовательно, должен быть защищен надлежащим образом, что важно для среды бизнеса, где наблюдается все возрастающая взаимосвязь. Как результат такой все возрастающей взаимосвязи, информация в настоящее время подвергается растущему числу и более широкому спектру угроз и уязвимостей (см. также Руководство ОЭСР[1)]) по обеспечению безопасности информационных систем и сетей [16].

Информация может существовать в различных формах: быть напечатанной или написанной на бумаге, храниться в электронном виде, передаваться по почте или с использованием электронных средств связи, демонстрироваться на пленке или выражена устно. Независимо от формы представления информации, средств ее распространения или хранения, она всегда должна быть адекватно защищена.

Информационная безопасность защищает информацию от широкого диапазона угроз с целью обеспечения уверенности в непрерывности бизнеса, минимизации риска бизнеса, получения максимальной отдачи от инвестиций, а также реализации потенциальных возможностей бизнеса.

Информационная безопасность достигается путем реализации соответствующего комплекса мер и средств контроля и управления, которые могут быть представлены политиками, процессами, процедурами, организационными структурами, а также функциями программных и аппаратных средств. Указанные меры и средства контроля и управления необходимо создавать, реализовывать, подвергать мониторингу, анализировать и улучшать, если необходимо, для обеспечения уверенности в том, что определенная безопасность и определенные цели бизнеса организации достигнуты. Все это необходимо выполнять наряду с другими процессами менеджмента бизнеса.

0.2 Почему необходима информационная безопасность?

Информация и поддерживающие ее процессы, системы и сети являются важными деловыми активами. Определение, достижение, поддержка и улучшение информационной безопасности могут быть существенными аспектами для поддержания конкурентоспособности, денежного оборота, доходности, соблюдения законов и коммерческого имиджа.

Организации, а также их информационные системы и сети сталкиваются с угрозами безопасности из широкого диапазона источников, включая компьютерное мошенничество, шпионаж, саботаж, вандализм, пожар или наводнение. Источники ущерба, например вредоносный код, компьютерное хакерство и атаки типа отказа в обслуживании, становятся более распространенными и все более и более изощренными.

Информационная безопасность важна как для государственного, так и для частного секторов бизнеса, а также для защиты критических инфраструктур. В обоих секторах информационная безопасность действует в качестве фактора, способствующего, например использованию «электронного правительства» или «электронного бизнеса», и чтобы избежать или снизить соответствующие риски. Взаимодействие сетей общего пользования и частных сетей, а также совместное использование информационных ресурсов приводит к увеличению трудностей, связанных с управлением доступом к информации. Тенденция к использованию распределенной обработки данных также ослабляет эффективность централизованного контроля.

При проектировании многих информационных систем проблемы безопасности не учитывались. Уровень безопасности, который может быть достигнут техническими средствами, имеет ряд ограничений и, следовательно, должен поддерживаться надлежащим менеджментом и процессами. Выбор необходимых мер и средств контроля и управления требует тщательного планирования и внимания к деталям. Менеджмент информационной безопасности нуждается, как минимум, в участии всех сотрудников организации. Кроме того, может потребоваться участие акционеров, поставщиков, представителей третьей стороны, клиентов или представителей других внешних сторон. Кроме того, могут потребоваться консультации специалистов сторонних организаций.

0.3 Как определить требования к информационной безопасности

Организация должна определить свои требования к информационной безопасности. Существуют три основных источника требований безопасности.

[1)] ОЭСР — организация экономического сотрудничества и развития (OECD — Organization for Economic Cooperation and Development).

Один из источников складывается из оценки рисков организации, принимая во внимание общую стратегию и цели бизнеса организации. Посредством оценки рисков идентифицируются угрозы активам организации, оцениваются уязвимости и вероятности возникновения угроз, а также оцениваются возможные последствия.

Вторым источником являются правовые, законодательные, нормативные и договорные требования, которым должны удовлетворять организация, ее торговые партнеры, подрядчики и поставщики услуг, а также их социокультурная среда.

Еще одним источником является определенный набор принципов, целей и требований бизнеса для обработки информации, которые разработала организация для поддержки своей деятельности.

0.4 Оценка рисков безопасности

Требования безопасности определяются с помощью систематической оценки рисков. Расходы на меры и средства контроля и управления должны быть соизмеримы с возможным ущербом бизнесу в результате отказа от обеспечения безопасности.

Результаты оценки рисков помогут в определении конкретных мер и приоритетов в области менеджмента рисков информационной безопасности, а также внедрению мер и средств контроля и управления, выбранных для защиты от этих рисков.

Оценка рисков должна периодически повторяться, чтобы учитывать любые изменения, которые могли бы повлиять на результаты оценки риска.

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

0.5 Выбор мер и средств контроля и управления

После того как были определены требования к безопасности и риски безопасности и приняты решения в отношении обработки рисков, следует выбрать и внедрить такие меры и средства контроля и управления, которые обеспечат уверенность в снижении рисков до приемлемого уровня. Меры и средства контроля и управления могут быть выбраны из настоящего документа и других источников, а также могут быть разработаны новые меры и средства контроля и управления, удовлетворяющие специфическим потребностям организации. Выбор мер и средств контроля и управления зависит от решений организации, основанных на критериях принятия рисков, вариантах обработки рисков и общем подходе к менеджменту рисков, применяемом в организации. При этом необходимо также учитывать все соответствующие национальные и международные законы и нормы.

Некоторые меры и средства контроля и управления, приведенные в настоящем документе, рекомендуется рассматривать как руководящие принципы для менеджмента информационной безопасности и применять для большинства организаций. Более подробно такие меры и средства контроля и управления рассматриваются ниже под заголовком «Отправная точка информационной безопасности».

Дополнительную информацию о выборе мер и средств контроля и управления и других вариантах обработки риска можно найти в 4.2 «Обработка рисков безопасности».

0.6 Отправная точка информационной безопасности

Отдельные меры и средства контроля и управления могут рассматриваться как подходящая отправная точка информационной безопасности. Такие меры и средства контроля и управления либо основываются на ключевых требованиях законодательства, либо рассматриваются как общепринятая практика в области информационной безопасности.

Ключевыми мерами и средствами контроля и управления, с точки зрения законодательства, для организации являются:

a) защита данных и конфиденциальность персональных данных (см. 15.1.4);

b) защита документов организации (см. 15.1.3);

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

Меры и средства контроля и управления, рассматриваемые как общепринятая практика в области информационной безопасности, включают:

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

b) распределение обязанностей по обеспечению информационной безопасности (см. 6.1.3);

c) осведомленность, обучение и тренинг[1)] в области информационной безопасности (см. 8.2.2);

[1)] Тренинг — обучение на практических занятиях или в приближенных к реальным условиях.

d) корректирующая обработка в прикладных программах (см. 12.2);

e) менеджмент технических уязвимостей (см. 12.6);

f) менеджмент непрерывности бизнеса (см. раздел 14);

g) менеджмент инцидентов информационной безопасности и необходимое совершенствование (см. 13.2).

Перечисленные меры и средства контроля и управления применимы для большинства организаций и сред.

Следует отметить, что хотя все меры и средства контроля и управления, приведенные в настоящем документе, являются важными, уместность какой-либо меры и средства контроля и управления должна определяться в свете конкретных рисков, с которыми сталкивается организация. Следовательно, несмотря на то, что вышеописанный подход рассматривается как отправная точка информационной безопасности, он не заменяет выбор мер и средств контроля и управления, основанный на оценке рисков.

0.7 Важнейшие факторы успеха

Практика показывает, что для успешного внедрения информационной безопасности в организации решающими факторами зачастую являются следующие:

a) соответствие целей, политик и процедур информационной безопасности целям бизнеса;

b) подход и основы для внедрения, поддержки, мониторинга и улучшения информационной безопасности, которые согласуются с корпоративной культурой;

c) видимая поддержка и обязательства со стороны руководства всех уровней;

d) четкое понимание требований информационной безопасности, оценки рисков и менеджмента рисков;

e) эффективный маркетинг информационной безопасности среди всех руководителей, сотрудников и других сторон для достижения осведомленности;

f) распространение руководящих указаний политики информационной безопасности и соответствующих стандартов среди всех руководителей, сотрудников и других сторон;

g) обеспечение финансирования деятельностей по менеджменту информационной безопасности;

h) обеспечение соответствующей осведомленности, обучения и тренинга;

i) создание эффективного процесса менеджмента инцидентов информационной безопасности;

j) внедрение системы измерений[1)], используемых для оценивания эффективности менеджмента информационной безопасности и предложений по улучшению.

0.8 Разработка собственных рекомендаций

Настоящий свод норм и правил может расцениваться как отправная точка для разработки рекомендаций, специфичных для организации. Не все рекомендации, меры и средства контроля и управления, приведенные в настоящем своде норм и правил, могут быть применимы. Более того, могут потребоваться дополнительные меры и средства контроля и управления и рекомендации, не включенные в данный документ. В документы, содержащие дополнительные рекомендации, а также меры и средства контроля и управления, в соответствующих случаях полезно включать перекрестные ссылки на положения настоящего стандарта для облегчения проверки соответствия, проводимой аудиторами и партнерами по бизнесу.

[1)] Обратите внимание на то, что измерения информационной безопасности не входят в сферу действия настоящего стандарта.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Свод норм и правил менеджмента информационной безопасности

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

Дата введения — 2014—01—01

1 Область применения

Настоящий национальный стандарт предлагает рекомендации и основные принципы введения, реализации, поддержки и улучшения менеджмента информационной безопасности в организации. Цели, изложенные в данном национальном стандарте, обеспечивают полное руководство по общепринятым целям менеджмента информационной безопасности.

Реализация целей управления, а также мер и средств контроля и управления настоящего национального стандарта направлена на удовлетворение требований, определенных оценкой рисков. Настоящий национальный стандарт может служить практическим руководством по разработке стандартов безопасности организации, для эффективной практики менеджмента безопасности организаций и способствует укреплению доверия в отношениях между организациями.

2 Термины и определения

В настоящем документе используются следующие термины с соответствующими определениями.

2.1

актив (asset): Все, что имеет ценность для организации.
[ИСО/МЭК 13335-1:2004]

2.2 **мера и средство контроля и управления** (control): Средство менеджмента риска, включающее в себя политики, процедуры, рекомендации, инструкции или организационные структуры, которые могут быть административного, технического, управленческого или правового характера.

Примечание — Термин «мера и средство контроля и управления» также используется как синоним терминов «защитная мера» (safeguard) или «контрмера» (countermeasure).

2.3

рекомендация (guideline): Описание, поясняющее действия и способы их выполнения, необходимые для достижения целей, изложенных в политике.
[ИСО/МЭК 13335-1:2004]

2.4 **средства обработки информации** (information processing facilities): Любая система обработки информации, услуга или инфраструктура, или их фактическое месторасположение.

2.5 **информационная безопасность** (information security): Защита конфиденциальности, целостности и доступности информации; кроме того, сюда могут быть отнесены и другие свойства, например аутентичность, подотчетность, неотказуемость и надежность.

Издание официальное

2.6

событие информационной безопасности (information security event): Какое-либо событие информационной безопасности, идентифицируемое появлением определенного состояния системы, сервиса или сети, указывающее на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

[ИСО/МЭК ТО 18044:2004]

2.7

инцидент информационной безопасности (information security incident): Какой-либо инцидент информационной безопасности, являющийся следствием одного или нескольких нежелательных или неожиданных событий информационной безопасности, которые имеют значительную вероятность компрометации операции бизнеса или создания угрозы информационной безопасности.

[ИСО/МЭК ТО 18044:2004]

2.8 **политика** (policy): Общее намерение и направление, официально выраженное руководством.

2.9

риск (risk): Сочетание вероятности события и его последствий.

[ИСО/МЭК Руководство 73:2002]

2.10

анализ риска (risk analysis): Систематическое использование информации для определения источников и количественной оценки риска.

[ИСО/МЭК Руководство 73:2002]

2.11

оценка риска (risk assessment): Общий процесс анализа риска и оценивания риска.

[ИСО/МЭК Руководство 73:2002]

2.12

оценивание риска (risk evaluation): Процесс сравнения количественно оцененного риска с заданными критериями риска для определения значимости риска.

[ИСО/МЭК Руководство 73:2002]

2.13

менеджмент риска (risk management): Скоординированные действия по руководству и управлению организацией в отношении риска.

Примечание — Обычно менеджмент риска включает в себя оценку риска, обработку риска, принятие риска и коммуникацию риска.

[ИСО/МЭК Руководство 73:2002]

2.14

обработка риска (risk treatment): Процесс выбора и осуществления мер по модификации риска.

[ИСО/МЭК Руководство 73:2002]

2.15

третья сторона (third party): Лица или организация, которые признаны независимыми от участвующих сторон, по отношению к рассматриваемой проблеме.

[ИСО/МЭК Руководство 2:1996]

2.16

угроза (threat): Потенциальная причина нежелательного инцидента, результатом которого может быть нанесение ущерба системе или организации.

[ИСО/МЭК 13335-1:2004]

2.17

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

[ИСО/МЭК 13335-1:2004]

3 Структура настоящего стандарта

Настоящий стандарт состоит из 11-ти разделов, посвященных мерам и средствам контроля и управления безопасности, которые все вместе содержат, в целом, 39 основных категорий безопасности, и одного вводного раздела, знакомящего с оценкой и обработкой рисков.

3.1 Разделы

В каждом разделе содержится несколько основных категорий безопасности. Этими одиннадцатью разделами (сопровождаемыми количеством основных категорий, включенных в каждый раздел) являются:

a) политика безопасности (1);

b) организационные аспекты информационной безопасности (2);

c) менеджмент активов (2);

d) безопасность, связанная с персоналом (3);

e) физическая защита и защита от воздействия окружающей среды (2);

f) менеджмент коммуникаций и работ (10);

g) управление доступом (7);

h) приобретение, разработка и эксплуатация информационных систем (6);

i) менеджмент инцидентов информационной безопасности (2);

j) менеджмент непрерывности бизнеса (1);

k) соответствие (3).

Примечание — Порядок расположения разделов в настоящем стандарте не подразумевает степень их важности. В зависимости от обстоятельств, все разделы могут быть важными, следовательно, каждой организации, использующей стандарт, следует определить применимые разделы, их важность, а также определить их применимость для отдельных процессов бизнеса. Все перечни, приведенные в настоящем стандарте, составлены без учета приоритетности, кроме случаев, оговоренных особо.

3.2 Основные категории безопасности

Каждая основная категория безопасности включает в себя:

a) цель управления, в которой формулируется, что должно быть достигнуто;

b) одну или более мер и средств контроля и управления, с помощью которых могут быть достигнуты цели управления.

Описания меры и средства контроля и управления структурируются следующим образом:

Мера и средство контроля и управления

Определяется формулировка специфической меры и средства контроля и управления для достижения цели управления.

Рекомендация по реализации

Предоставляется более детализированная информация для поддержки реализации меры и средства контроля и управления и достижения цели управления. Некоторые из этих рекомендаций могут быть неприемлемы для всех случаев, поэтому другие способы реализации меры и средства контроля и управления могут быть более уместными.

Дополнительная информация

Предоставляется дополнительная информация, которая может быть рассмотрена, например правовые вопросы и ссылки на другие стандарты.

4 Оценка и обработка рисков

4.1 Оценка рисков безопасности

Оценка рисков должна идентифицировать риски, определить количество и приоритеты рисков на основе критериев для принятия риска и целей, значимых для организации. Результаты должны служить ориентиром и определять соответствующие действия руководства и приоритеты менеджмента рисков инфор-

мационной безопасности, а также реализацию мер и средств контроля и управления, выбранных для защиты от этих рисков. Может возникнуть необходимость в неоднократном выполнении процесса оценки рисков и выбора мер и средств контроля и управления для того, чтобы охватить различные подразделения организации или отдельные информационные системы.

Оценка рисков должна включать систематический подход, заключающийся в количественной оценке рисков (анализ риска), и процесс сравнения количественно оцененных рисков с данными критериями рисков для определения значимости рисков (оценивание рисков).

Оценки рисков следует выполнять периодически, чтобы учитывать изменения в требованиях безопасности и в ситуации, связанной с риском, например в отношении активов, угроз, уязвимостей, воздействий, оценивания рисков, а также при значительных изменениях. Такие оценки рисков следует проводить систематически, способом, дающим сравнимые и воспроизводимые результаты.

Чтобы быть эффективной, оценка рисков информационной безопасности должна иметь четко определенную область применения и, при необходимости, взаимосвязь с оценками рисков в других областях.

Областью применения оценки рисков может быть целая организация, ее подразделения, отдельная информационная система, определенные компоненты системы, или услуги, где это возможно, реально и полезно. Примеры методик оценки рисков рассматриваются в ИСО/МЭК ТО 13335-3 [4].

4.2 Обработка рисков безопасности

Прежде чем рассмотреть обработку некоего риска, организация должна выбрать критерии определения приемлемости или неприемлемости рисков. Риски могут быть приняты, если, например они оцениваются как низкие, или когда стоимость обработки невыгодна для организации. Такие решения необходимо регистрировать.

В отношении каждого из выявленных рисков, вслед за оценкой рисков, необходимо принимать решение по его обработке. Возможные варианты обработки рисков включают в себя:

a) применение соответствующих мер и средств контроля и управления для снижения рисков;

b) сознательное и объективное принятие рисков в том случае, если они, несомненно, удовлетворяют политике и критериям организации в отношении принятия рисков;

c) предотвращение рисков путем недопущения действий, которые могут стать причиной возникновения рисков;

d) перенос взаимодействующих рисков путем разделения их с другими сторонами, например страховщиками или поставщиками.

Что касается тех рисков, в отношении которых было принято решение об их обработке с применением соответствующих мер и средств контроля и управления, эти меры и средства контроля и управления следует выбирать и реализовывать таким образом, чтобы они соответствовали требованиям, идентифицированным оценкой рисков. Меры и средства контроля и управления должны обеспечивать уверенность в том, что эти риски снижены до приемлемого уровня, принимая во внимание:

a) требования и ограничения национальных и международных законов и норм;

b) цели организации;

c) эксплуатационные требования и ограничения;

d) стоимость реализации и эксплуатации в отношении снижаемых рисков должна оставаться пропорциональной требованиям и ограничениям организации;

e) необходимость сохранения баланса между инвестициями в реализацию и эксплуатацию мер и средств контроля и управления и ущербом, который может иметь место в результате недостаточной безопасности.

Меры и средства контроля и управления могут быть выбраны из настоящего стандарта или других совокупностей мер и средств контроля и управления, могут быть созданы новые меры и средства контроля и управления с целью удовлетворения специфических потребностей организации. Необходимо признать, что некоторые меры и средства контроля и управления не могут быть применены для каждой информационной системы или среды, и не могут быть применены для всех организаций. В качестве примера, в 10.1.3 описывается, как обязанности могут быть разделены, чтобы предотвратить мошенничество и ошибки. В небольших организациях может отсутствовать возможность разделения всех обязанностей, и могут потребоваться другие способы достижения той же самой цели управления. В качестве другого примера в 10.10 описывается способ осуществления мониторинга работы системы и сбора доказательств. Описанные меры и средства контроля и управления, например регистрация событий, могут вступать в противоречие с действующим законодательством, например по обеспечению конфиденциальности в отношении клиентов или на рабочем месте.

Меры и средства контроля и управления информационной безопасности должны рассматриваться на этапе спецификации и разработки системных и проектных требований. Отказ от этого может приводить к дополнительным расходам и менее эффективным решениям, а в худшем случае, к неспособности достижения адекватной безопасности.

Следует иметь в виду, что никакая совокупность мер и средств контроля и управления не может достигать полной безопасности, и что необходимо реализовывать дополнительные действия по менеджменту, чтобы осуществлять мониторинг, оценку и повышение действенности и эффективности мер и средств контроля и управления безопасности для поддержки целей организации.

5 Политика безопасности

5.1 Политика информационной безопасности

Цель: Обеспечить управление и поддержку высшим руководством информационной безопасности в соответствии с требованиями бизнеса и соответствующими законами и нормами.

Высшее руководство должно установить четкое направление политики в соответствии с целями бизнеса и демонстрировать поддержку и обязательства в отношении обеспечения информационной безопасности посредством разработки и поддержки политики информационной безопасности в рамках организации.

При необходимости следует предусмотреть наличие контактного лица, занимающегося вопросами информационной безопасности внутри организации, к которому могут обращаться заинтересованные сотрудники. Следует налаживать контакты с внешними специалистами по безопасности или группами специалистов, включая соответствующие органы, чтобы находиться в курсе отраслевых тенденций, осуществлять мониторинг стандартов и методов оценки, и обеспечивать адекватные точки контакта при обработке инцидентов информационной безопасности. Следует поощрять многопрофильный подход к обеспечению информационной безопасности.

5.1.1 Документирование политики информационной безопасности

Мера и средство контроля и управления

Политика информационной безопасности должна быть утверждена руководством, издана и доведена до сведения всех сотрудников организации и соответствующих сторонних организаций.

Рекомендация по реализации

Политика информационной безопасности должна устанавливать ответственность руководства, а также излагать подход организации к менеджменту информационной безопасности. Документ, в котором излагается политика, должен содержать положения относительно:

a) определения информационной безопасности, ее общих целей и сферы действия, а также упоминания значения безопасности как инструмента, обеспечивающего возможность совместного использования информации (см. «Введение»);

b) изложения намерений руководства, поддерживающих цели и принципы информационной безопасности в соответствии со стратегией и целями бизнеса;

c) подхода к установлению мер и средств контроля и управления и целей их применения, включая структуру оценки риска и менеджмента риска;

d) краткого разъяснения наиболее существенных для организации политик безопасности, принципов, стандартов и требований соответствия, например:

1) соответствие законодательным требованиям и договорным обязательствам;

2) требования по обеспечению осведомленности, обучения и тренинга в отношении безопасности;

3) менеджмент непрерывности бизнеса;

4) ответственность за нарушения политики информационной безопасности;

e) определения общих и конкретных обязанностей сотрудников в рамках менеджмента информационной безопасности, включая информирование об инцидентах безопасности;

f) ссылок 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.

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

Дополнительная информация

Политика информационной безопасности может составлять часть документа по общей политике. Если политика информационной безопасности распространяется за пределами организации, следует принимать меры в отношении неразглашения чувствительной информации. Дополнительную информацию можно найти в ИСО/МЭК 13335-1 [3].

5.1.2 Пересмотр политики информационной безопасности

Мера и средство контроля и управления

Политика информационной безопасности должна пересматриваться либо через запланированные интервалы времени, либо, если произошли значительные изменения, с целью обеспечения уверенности в ее актуальности, адекватности и эффективности.

Рекомендация по реализации

Политика информационной безопасности должна иметь владельца, который утвержден руководством в качестве ответственного за разработку, пересмотр и оценку политики безопасности. Пересмотр заключается в оценке возможностей по улучшению политики информационной безопасности организации и подхода к менеджменту информационной безопасности в ответ на изменения организационной среды, обстоятельств бизнеса, правовых условий или технической среды.

При пересмотре политики информационной безопасности следует учитывать результаты пересмотров методов управления. Должны существовать определенные процедуры пересмотра методов управления, в том числе график или период пересмотра.

Входные данные для пересмотра методов управления должны включать информацию об (о):

a) ответной реакции заинтересованных сторон;

b) результатах независимых пересмотров (см. 6.1.8);

c) состоянии предотвращающих и корректирующих действий (см. 6.1.8 и 15.2.1);

d) результатах предыдущих пересмотров методов управления;

e) выполнении процесса и соответствии политике информационной безопасности;

f) изменениях, которые могли бы повлиять на подход организации к методам управления информационной безопасностью, включая изменения, касающиеся организационной среды, обстоятельств бизнеса, доступности ресурсов, контрактных, регулирующих и правовых условий или технической среды;

g) тенденциях в отношении угроз и уязвимостей;

h) доведенных до сведения инцидентах информационной безопасности (см. 13.1);

i) рекомендациях, данных соответствующими органами (см. 6.1.6).

Выходные данные пересмотра методов управления должны включать любые решения и действия относительно:

a) улучшения подхода организации к менеджменту информационной безопасности и ее процессов;

b) улучшения мер и средств контроля и управления и целей их применения;

c) улучшения распределения ресурсов и (или) обязанностей.

Пересмотр методов управления следует документировать.

Пересмотренная политика должна быть утверждена руководством.

6 Организационные аспекты информационной безопасности

6.1 Задачи, решаемые внутри организации

Цель: Осуществлять менеджмент информационной безопасности в рамках организации.

Должна быть создана структура менеджмента для инициирования и контроля обеспечения информационной безопасности в организации.

Высшее руководство должно утверждать политику информационной безопасности организации, назначать ответственных лиц в области политики информационной безопасности, а также координировать и анализировать внедрение информационной безопасности в организации.

При необходимости следует предусмотреть наличие контактного лица, занимающегося вопросами информационной безопасности внутри организации, к которому могут обращаться заинтересованные сотрудники. Следует налаживать контакты с отдельными внешними специалистами по безопасности или группами специалистов, включая соответствующие органы, чтобы находиться в курсе отраслевых тенденций, осуществлять мониторинг стандартов и методов оценки, и обеспечивать адекватные точки контакта при обработке инцидентов информационной безопасности. Следует поощрять многопрофильный подход к обеспечению информационной безопасности.

6.1.1 Обязательства руководства по отношению к информационной безопасности

Мера и средство контроля и управления

Руководству следует активно поддерживать безопасность в организации с помощью четкого управления, видимого распределения обязанностей, определенных назначений и признания обязанностей в отношении информационной безопасности.

Рекомендация по реализации

Руководству следует:

a) обеспечивать уверенность в том, что цели информационной безопасности определены, соответствуют требованиям организации и включены в соответствующие процессы;

b) формулировать, анализировать и утверждать политику информационной безопасности;

c) анализировать эффективность реализации политики информационной безопасности;

d) обеспечивать четкое управление и очевидную поддержку менеджмента в отношении инициатив, связанных с безопасностью;

e) обеспечивать ресурсы, необходимые для информационной безопасности;

f) утверждать определенные роли и ответственности в отношении информационной безопасности в рамках организации;

g) инициировать планы и программы для поддержки осведомленности об информационной безопасности;

h) обеспечивать уверенность в том, что реализация мер и средств контроля и управления информационной безопасности скоординирована в рамках организации (см. 6.1.2).

Руководству следует определять потребность в консультациях с внутренними или внешними специалистами по информационной безопасности, а также анализировать и координировать результаты консультаций в рамках организации.

В зависимости от величины организации такие обязанности могут выполняться специальным административным совещанием или существующим органом управления, например советом директоров.

Дополнительная информация

Дополнительная информация содержится в ИСО/МЭК 13335-1 [3].

6.1.2 Координация вопросов информационной безопасности

Мера и средство контроля и управления

Деятельность, связанная с информационной безопасностью, должна быть скоординирована представителями различных подразделений организации с соответствующими ролями и должностными обязанностями.

Рекомендация по реализации

Как правило, координация проблем информационной безопасности должна включать в себя сотрудничество и участие менеджеров, пользователей, администраторов, разработчиков прикладных программ, аудиторов и персонала, занимающегося безопасностью, а также специалистов в области страхования, правовых аспектов, кадровых ресурсов, ИТ или менеджмента риска.

Такая деятельность должна:

a) обеспечивать уверенность в том, что обеспечение безопасности осуществляется в соответствии с политикой информационной безопасности;

b) определять способ устранения несоответствия;

c) утверждать методики и процессы обеспечения информационной безопасности, например оценку риска, классификацию информации;

d) выявлять значительные изменения угроз и подверженность информации и средств обработки информации угрозам;

e) оценивать адекватность и координировать реализацию мер и средств контроля и управления информационной безопасности;

f) эффективно способствовать осведомленности, обучению и тренингу в отношении информационной безопасности в рамках организации;

g) оценивать информацию, полученную в результате мониторинга и анализа инцидентов информационной безопасности, и рекомендовать соответствующие действия в ответ на выявленные инциденты информационной безопасности.

Если в организации не используется специальная межфункциональная группа, например по причине несоответствия величине организации, вышеописанные действия могут выполняться другим подходящим органом управления или отдельным менеджером.

6.1.3 Распределение обязанностей по обеспечению информационной безопасности

Мера и средство контроля и управления

Все обязанности по обеспечению информационной безопасности должны быть четко определены.

Рекомендация по реализации

Распределение обязанностей по обеспечению информационной безопасности следует осуществлять в соответствии с политикой информационной безопасности (см. 4). Следует четко определять обязанности по защите отдельных активов и по выполнению конкретных процессов, связанных с информационной безопасностью. Такие обязанности следует дополнять, при необходимости, более детальными руководствами для конкретных мест эксплуатации и средств обработки информации. Конкретные обязанности в отношении защиты активов и осуществления специфических процессов, связанных с безопасностью, например планирование непрерывности бизнеса, должны быть четко определены.

Лица, на которые возложена обязанность по обеспечению безопасности, могут делегировать задачи, связанные с безопасностью, другим лицам. Тем не менее, они остаются ответственными за выполнение делегированных задач.

Круг обязанностей каждого руководителя должен быть четко определен, в частности:

a) активы и процессы (процедуры) безопасности, связанные с каждой конкретной системой, должны быть четко определены;

b) необходимо назначить ответственных за каждый актив или процедуру безопасности, и подробно описать их обязанности в соответствующих документах (см. 7.1.2);

c) уровни полномочий должны быть четко определены и документально оформлены.

Дополнительная информация

Во многих организациях назначается менеджер по информационной безопасности, на которого возлагается общая ответственность за разработку и реализацию безопасности и за поддержку определения мер и средств контроля и управления.

Однако обязанности в отношении поиска ресурсов и реализации мер и средств контроля и управления часто вменяются отдельным менеджерам. Общепринятой практикой является назначение владельца для каждого актива, который несет ответственность за его повседневную защиту.

6.1.4 Процесс получения разрешения на использование средств обработки информации

Мера и средство контроля и управления

Необходимо определить и реализовать процесс получения разрешения у руководства на использование новых средств обработки информации.

Рекомендация по реализации

В отношении процесса получения разрешения следует рассмотреть следующие рекомендации:

a) на новые средства должны быть получены соответствующие разрешения руководства пользователей, утверждающего их цель и использование. Разрешение следует также получать от менеджера, ответственного за поддержку среды безопасности локальной информационной системы, чтобы обеспечить уверенность в том, что все соответствующие требования и политики безопасности соблюдаются;

b) аппаратные средства и программное обеспечение, где необходимо, следует проверять на предмет совместимости с другими компонентами системы;

c) использование персональных или находящихся в частной собственности средств обработки информации, например лэптопов, домашних компьютеров или карманных устройств для обработки деловой информации может являться причиной новых уязвимостей, поэтому следует определять и реализовывать необходимые меры и средства контроля и управления.

6.1.5 Соглашения о конфиденциальности

Мера и средство контроля и управления

Требования в отношении соглашений о конфиденциальности или неразглашении, отражающие потребности организации в защите информации, должны определяться и регулярно пересматриваться.

Рекомендация по реализации

В соглашениях о конфиденциальности или неразглашении должно содержаться требование о защите конфиденциальной информации, выраженное юридическими терминами, имеющими исковую силу. Чтобы определить требования для соглашений о конфиденциальности или неразглашении, необходимо учесть следующие факторы:

a) определение информации, подлежащей защите (например конфиденциальная информация);

b) предполагаемый срок действия соглашения, включая случаи, когда может возникнуть необходимость в неограниченной поддержке конфиденциальности;

c) необходимые действия при окончании срока действия соглашения;

d) обязанности и действия лиц, подписавших соглашение, с целью предотвращения несанкционированного разглашения информации (например по принципу «необходимого знания»);

e) владение информацией, коммерческие тайны и интеллектуальная собственность, и как это соотносится с защитой конфиденциальной информации;

f) разрешенное использование конфиденциальной информации и права лиц, подписавших соглашение, в отношении использования информации;

g) право подвергать аудиту и мониторингу деятельность, связанную с конфиденциальной информацией;

h) процедуру предупреждения и сообщения о несанкционированном разглашении или нарушениях, связанных с конфиденциальной информацией;

i) условия возврата или уничтожения информации в случае приостановления действия соглашения;

j) предполагаемые действия, которые должны быть предприняты в случае нарушения данного соглашения.

В зависимости от требований безопасности организации, могут потребоваться дополнительные элементы соглашения о конфиденциальности или неразглашении.

Соглашения о конфиденциальности и неразглашении должны соответствовать всем применимым законам и нормам, под юрисдикцию которых они подпадают (см. 15.1.1).

Требования в отношении соглашений о конфиденциальности и неразглашении должны пересматриваться периодически и когда происходят изменения, влияющие на эти требования.

Дополнительная информация

Соглашения о конфиденциальности и неразглашении защищают информацию организации, а также информируют лиц, подписавших соглашение, об их обязанности защищать, использовать и разглашать информацию внушающим доверие и санкционированным способом.

При различных обстоятельствах организации могут потребоваться различные формы соглашений о конфиденциальности или неразглашении.

6.1.6 Контакт с различными инстанциями

Мера и средство контроля и управления

Должны поддерживаться соответствующие контакты с различными инстанциями.

Рекомендация по реализации

В организациях должны применяться процедуры, определяющие, когда и с какими инстанциями (например правоохранительными, пожарными и надзорными органами) необходимо вступить в контакт, и каким образом следует своевременно сообщать о выявленных инцидентах информационной безопасности, если есть подозрение о возможности нарушения закона.

Организациям, подвергающимся атаке через Интернет, может потребоваться привлечение внешней третьей стороны (например провайдера Интернет-услуг или телекоммуникационного оператора) для принятия мер против источника атаки.

Дополнительная информация

При осуществлении таких контактов может потребоваться поддержка процесса менеджмента инцидентов информационной безопасности (см. 13.2) или процесса планирования непрерывности бизнеса и действий в чрезвычайных ситуациях (см. 14). Также следует поддерживать контакты с регулирующими органами для прогнозирования и подготовки к предстоящим изменениям в законах или нормах, которые должны соблюдаться организацией. Контакты с другими инстанциями включают контакты с коммунальными службами, скорой помощью и службами охраны труда, например с пожарными органами (в связи с непрерывностью бизнеса), провайдерами телекоммуникационных услуг (в связи с трассировкой линий связи и их доступностью), службами водоснабжения (в связи со средствами охлаждения оборудования).

6.1.7 Контакт со специализированными профессиональными группами

Мера и средство контроля и управления

Должны поддерживаться соответствующие контакты со специализированными профессиональными группами или участниками форумов по безопасности, а также с профессиональными ассоциациями.

Рекомендация по реализации

Членство в специализированных группах или форумах следует рассматривать как средство для:

a) повышения знания о «передовом опыте» и достижений информационной безопасности на современном уровне;

b) обеспечения уверенности в том, что понимание проблем информационной безопасности является современным и полным;

c) получения раннего оповещения в виде предупреждений, информационных сообщений и патчей[1)], касающихся атак и уязвимостей;

d) возможности получения консультаций специалистов по вопросам информационной безопасности;

e) совместного использования и обмена информацией о новых технологиях, продуктах, угрозах или уязвимостях;

f) обеспечения адекватных точек контакта для обсуждения инцидентов информационной безопасности (см. 13.2.1).

Дополнительная информация

Могут быть установлены соглашения на совместное использование информации с целью улучшения сотрудничества и координации по вопросам безопасности. В таких соглашениях должны быть определены требования в отношении защиты чувствительной информации.

6.1.8 Независимая проверка информационной безопасности

Мера и средство контроля и управления

Подход организации к менеджменту информационной безопасности и ее реализации (т. е. цели управления, политики, процессы и процедуры по обеспечению информационной безопасности) должен проверяться независимым образом через запланированные интервалы времени, или когда произошли значительные изменения, связанные с реализацией безопасности.

Рекомендация по реализации

Независимая проверка должна инициироваться руководством. Такая независимая проверка необходима для обеспечения уверенности в сохраняющейся работоспособности, адекватности и эффективности подхода организации к менеджменту информационной безопасности. Проверка должна включать в себя оценку возможностей улучшения и необходимость изменений подхода к безопасности, в том числе политику и цели управления.

Такая проверка должна осуществляться специалистами, не работающими в рассматриваемой области деятельности, например службой внутреннего аудита, независимым менеджером или сторонней организацией, специализирующейся на таких проверках. Специалисты, привлекаемые к таким проверкам, должны обладать соответствующими навыками и опытом.

Результаты независимой проверки должны регистрироваться и сообщаться руководству, инициировавшему проверку. Эти отчеты необходимо сохранять для возможного последующего использования.

Если в результате независимой проверки устанавливается, что подход организации и реализация менеджмента информационной безопасности неадекватны или не соответствуют направлению информационной безопасности, изложенному в документе, содержащем политику информационной безопасности (см. 5.1.1), руководству следует рассмотреть соответствующие корректирующие действия.

Дополнительная информация

Область деятельности, которую менеджеры должны регулярно проверять (см. 15.2.1), может быть проверена независимым образом. Методы проверки могут включать опрос руководства, проверку данных регистрации или анализ документов, имеющих отношение к политике безопасности. ИСО 19011 [15] также может предоставить полезное руководство по выполнению независимой проверки, включая создание и реализацию программы проверки. В 15.3 определены меры и средства контроля и управления, имеющие значение для независимой проверки эксплуатируемых информационных систем и использования инструментальных средств аудита.

6.2 Аспекты взаимодействия со сторонними организациями

Цель: Обеспечивать безопасность информации и средств обработки информации организации при доступе, обработке, передаче и менеджменте, осуществляемом сторонними организациями.

Безопасность информации и средств обработки информации организации не должна снижаться при вводе продуктов или сервисов сторонних организаций.

Доступ сторонних организаций к средствам обработки информации организации, а также к обработке и передаче информации должен находиться под контролем.

[1)] Патч — блок изменений для оперативного исправления или нейтрализации ошибки в исполняемой программе, чаще всего поставляемый (или размещаемый на сайте разработчика) в виде небольшой программы, вставляющей исправления в объектный код соответствующих модулей приложения. Иногда этот метод используется для добавления в приложение новой функциональности.

Если имеется потребность бизнеса в работе со сторонними организациями, которым может потребоваться доступ к информации и средствам обработки информации организации, а также в получении или обеспечении продукта или сервиса от сторонней организации или для нее, следует выполнять оценку риска для определения последствий для безопасности и требований к мерам и средствам контроля и управления. Меры и средства контроля и управления следует согласовывать и определять в контракте со сторонней организацией

6.2.1 Идентификация рисков, являющихся следствием работы со сторонними организациями

Мера и средство контроля и управления

Риски для информации и средств обработки информации организации, являющиеся следствием процессов бизнеса, в которых участвуют сторонние организации, необходимо определять и необходимо реализовывать соответствующие меры и средства контроля и управления прежде, чем будет предоставлен доступ.

Рекомендация по реализации

Там, где есть необходимость разрешения доступа сторонней организации к средствам обработки информации или информации организации, следует проводить оценку риска (см. 4) с целью определения каких-либо потребностей в специальных мерах и средствах контроля и управления. При определении рисков, связанных с доступом сторонних организаций, следует учитывать:

a) средства обработки информации, необходимые сторонним организациям для доступа;

b) тип доступа к информации и средствам обработки информации, который будет предоставлен сторонним организациям, например:

1) физический доступ, например к офисам, машинным залам, картотекам;

2) логический доступ, например к базам данных, информационным системам организации;

3) возможность сетевого соединения между сетью (сетями) организации и сторонней организации, например неразъемное соединение, удаленный доступ;

4) осуществление доступа на месте или вне места эксплуатации;

c) ценность и чувствительность используемой информации, ее критичность для операций бизнеса;

d) меры и средства контроля и управления, необходимые для защиты информации, не предназначенной для доступа сторонним организациям;

e) персонал сторонней организации, участвующий в обработке информации организации;

f) каким образом организация или персонал, авторизованные на получение доступа, могут быть идентифицированы, авторизация проверена и как часто это необходимо подтверждать;

g) различные способы и меры и средства контроля и управления, применяемые сторонними организациями при хранении, обработке, передаче, совместном использовании и обмене информацией;

h) влияние непредоставления требуемого доступа сторонней организации и ввода или получения сторонней организацией неточной или ложной информации;

i) инструкции и процедуры принятия мер в отношении инцидентов информационной безопасности и возможных убытков, а также сроки и условия возобновления доступа сторонних организаций в случае инцидента информационной безопасности;

j) правовые и нормативные требования, а также договорные обязательства, значимые для сторонних организаций, которые необходимо принимать в расчет;

k) влияние вышеназванных мер на интересы каких-либо других причастных сторон.

Доступ сторонних организаций к информации организации не должен обеспечиваться до тех пор, пока не будут реализованы соответствующие меры и средства контроля и управления и пока не будет подписан договор, определяющий сроки и условия подключения или доступа и рабочий механизм. Как правило, все требования к безопасности, вытекающие из работы со сторонними организациями или внутреннего контроля, должны отражаться в соглашении со сторонними организациями (см. 6.2.2 и 6.2.3).

Следует обеспечивать уверенность в том, что сторонние организации осведомлены о своих обязанностях, и берут на себя ответственность и обязательства в отношении доступа, обработки, передачи или менеджмента информации и средств обработки информации организации.

Дополнительная информация

Информация может быть подвергнута риску сторонними организациями, в которых менеджмент безопасности осуществляется неадекватным образом. Должны определяться и применяться меры и средства контроля и управления с целью администрирования доступа сторонней организации к средствам обработки информации. Например там, где имеется определенная потребность в конфиденциальности информации, могут быть использованы соглашения о неразглашении.

Организации могут сталкиваться с рисками, связанными с межорганизационными процессами, менеджментом и связью в том случае, если применяется большой процент аутсорсинга[1)], или если к участию привлекаются несколько сторонних организаций.

Меры и средства контроля и управления, приведенные в 6.2.2 и 6.2.3, охватывают различные мероприятия с привлечением сторонних организаций, включающие:

a) провайдеров услуг, например Интернет-провайдеров, сетевых провайдеров, услуги телефонной связи, технического обслуживания и поддержки;

b) услуги по менеджменту безопасности;

c) клиентов;

d) аутсорсинг средств и (или) операций, например систем ИТ, услуг по сбору данных, операций центра телефонного обслуживания;

e) консультантов по вопросам менеджмента и бизнеса, а также аудиторов;

f) разработчиков и поставщиков, например программных продуктов и систем ИТ;

g) уборку, общественное питание и другие вспомогательные услуги, обеспечиваемые в рамках договоров аутсорсинга;

h) временных работников, прием на работу студентов и другие нерегулярные краткосрочные назначения.

Такие соглашения могут помочь снизить риски, связанные с привлечением сторонних организаций.

6.2.2 Рассмотрение вопросов безопасности при работе с клиентами

Мера и средство контроля и управления

Все установленные требования безопасности должны быть рассмотрены прежде, чем клиентам будет дан доступ к информации или активам организации.

Рекомендация по реализации

Следующие условия должны быть учтены при рассмотрении безопасности до предоставления клиентам доступа к какому-либо активу организации (в зависимости от типа и продолжительности предоставляемого доступа не все из них могут быть применимы):

a) защита активов, включая:

1) процедуры защиты активов организации, в том числе информацию и программное обеспечение, а также менеджмент известных уязвимостей;

2) процедуры для определения компрометации активов, например вследствие потери или модификации данных;

3) целостность;

4) ограничения на копирование и разглашение информации;

b) описание продукта или услуги, которые должны быть обеспечены;

c) различные причины, требования и преимущества, связанные с доступом клиента;

d) политика управления доступом, охватывающая:

1) разрешенные методы доступа, а также управление и использование уникальных идентификаторов, типа идентификаторов пользователя и паролей;

2) процесс авторизации в отношении доступа и привилегий пользователей;

3) положение о том, что весь доступ, не авторизованный явным образом, является запрещенным;

4) процесс отмены прав доступа или прерывание соединения между системами;

e) процедуры в отношении отчетности, уведомления и расследования неточностей в информации (например персональных подробностей), инцидентов информационной безопасности и нарушений безопасности;

f) описание каждой предоставляемой услуги;

g) определение необходимого и неприемлемого уровня обслуживания;

h) право на проведение мониторинга и отмену какой-либо деятельности, связанной с активами организации;

i) соответствующие обязательства организации и клиента;

j) обязательства относительно юридических вопросов, и способ обеспечения уверенности в соответствии правовым нормам, например законодательству о защите данных, особенно с учетом различных

[1)] Аутсорсинг — привлечение внешних организаций (на договорной основе) для выполнения некоторых бизнес-функций или частей бизнес-процесса организации.

требований национальных правовых систем, если договор предполагает сотрудничество с клиентами в других странах (см. 15.1);

k) соблюдение прав на интеллектуальную собственность и авторских прав (см. 15.1.2), а также обеспечение правовой защиты любой совместной работы (см. 6.1.5).

Дополнительная информация

Требования безопасности в отношении клиентов, осуществляющих доступ к активам организации, могут варьироваться в значительной степени в зависимости от средств обработки информации и информации, к которой осуществляется доступ. Такие требования безопасности могут быть рассмотрены с использованием договоров с клиентами, в которых содержатся все установленные риски и требования безопасности (см. 6.2.1).

По договорам со сторонними организациями могут также привлекаться другие участники. В договорах, предоставляющих доступ сторонней организации, должно содержаться разрешение на привлечение других организаций, а также условия их доступа и участия.

6.2.3 Рассмотрение требований безопасности в договорах с третьей стороной

Мера и средство контроля и управления

Договоры с третьей стороной, привлеченной к доступу, обработке, передаче или управлению информацией или средствами обработки информации организации, или к дополнению продуктов или услуг к средствам обработки информации, должны охватывать все соответствующие требования безопасности.

Рекомендация по реализации

Договор должен обеспечивать уверенность в том, что нет никакого недопонимания между организацией и третьей стороной. Организации должны убедиться, что третья сторона сможет возместить возможные убытки.

Следующие условия должны быть рассмотрены на предмет включения в договор с целью удовлетворения установленных требований безопасности (см. 6.2.1):

a) политика информационной безопасности;

b) меры и средства контроля и управления для обеспечения уверенности в защите активов, включая:

1) процедуры по защите активов организации, в том числе информацию, программное обеспечение и аппаратные средства;

2) какие-либо меры и средства контроля и управления, а также инструменты необходимой физической защиты;

3) меры и средства контроля и управления для обеспечения уверенности в защите от вредоносного программного средства (см. 10.4.1);

4) процедуры по определению компрометации активов, например вследствие потери или модификации информации, программного обеспечения и аппаратных средств;

5) меры и средства контроля и управления по обеспечению уверенности в возврате или уничтожении информации и активов по окончании договора или в согласованное время в течение срока действия договора;

6) конфиденциальность, целостность, доступность и любое другое значимое свойство (см. пункт 2.5) активов;

7) ограничения на копирование и разглашение информации, и применение соглашений о конфиденциальности (см. 6.1.5);

c) тренинг пользователей и администраторов в отношении методов, процедур и безопасности;

d) обеспечение осведомленности пользователей в отношении обязанностей и вопросов, связанных с информационной безопасностью;

e) обеспечение доставки персонала к месту работы, где это необходимо;

f) обязанности, касающиеся установки и сопровождения аппаратных средств и программного обеспечения;

g) четкая структура подотчетности и согласованные форматы представления отчетов;

h) ясный и определенный процесс менеджмента изменений;

i) политика управления доступом, охватывающая:

1) различные причины, требования и преимущества, делающие доступ третьей стороны необходимым;

2) разрешенные методы доступа, а также управление и использование уникальных идентификаторов типа идентификаторов пользователя и паролей;

3) процесс авторизации в отношении доступа и привилегий пользователей;

4) требование по ведению списка лиц, уполномоченных использовать предоставляемые услуги, с указанием соответствующих прав и привилегий;

5) положение о том, что весь доступ, не авторизованный явным образом, является запрещенным;

6) процесс отмены прав доступа или прерывание соединения между системами;

j) процедуры в отношении отчетности, уведомления и расследования инцидентов информационной безопасности и нарушений безопасности, а также нарушений требований, изложенных в соглашении;

k) описание продукта или услуги, которые должны быть предоставлены, и описание информации, которая должна быть предоставлена, наряду с категорией ее секретности (см. 7.2.1);

l) определение необходимого и неприемлемого уровня обслуживания;

m) определение поддающихся контролю критериев эффективности, а также их мониторинг и предоставление отчетности;

n) право на проведение мониторинга и отмену любой деятельности в отношении активов организации;

o) право на проведение аудита исполнения договорных обязательств и возможность проведения такого аудита третьей стороной, а также перечисление установленных законом прав аудиторов;

p) установление процесса информирования о возникающих проблемах с целью их разрешения;

q) требования в отношении непрерывности обслуживания, включая меры по обеспечению доступности и надежности, в соответствии с приоритетами бизнеса организации;

r) соответствующие обязательства сторон в рамках соглашения;

s) обязательства относительно юридических вопросов, и способов обеспечения уверенности в соответствии правовым требованиям, например законодательству о защите данных, особенно с учетом различных требований национальных правовых систем, если договор предполагает сотрудничество с клиентами в других странах (см. также 15.1);

t) соблюдение прав на интеллектуальную собственность и авторских прав (см. 15.1.2), а также обеспечение правовой защиты любой совместной работы (см. 6.1.5);

u) привлечение третьей стороны вместе с субподрядчиками, меры и средства контроля и управления безопасности, которые эти субподрядчики должны реализовать;

v) условия перезаключения/окончания договоров:

1) план действий в чрезвычайных ситуациях должен содержать положения на случай, если какая-либо сторона пожелает прервать отношения до окончания срока действия договоров;

2) перезаключение договоров в случае изменения требований организации к безопасности;

3) действующие документированные перечни активов, лицензий, договоров или связанных с ними прав.

Дополнительная информация

Договоры могут варьироваться в значительной мере в отношении различных организаций и среди различных типов третьих сторон. Поэтому следует заботиться о включении в договоры всех определенных рисков и требований безопасности (см. также 6.2.1). При необходимости требуемые меры и средства контроля и управления, а также процедуры могут быть расширены в плане менеджмента безопасности.

Если менеджмент информационной безопасности осуществляется в рамках договоров аутсорсинга, то в договорах должно быть оговорено, каким образом третья сторона будет гарантировать поддержание адекватной безопасности, определенной оценкой риска, а также адаптацию к выявленным рискам и изменениям рисков.

Некоторые из различий между аутсорсингом и другими формами обеспечения услуг третьими сторонами включают в себя вопросы ответственности, планирование переходного периода и возможного срыва операций в течение данного периода, планирование мероприятий на случай непредвиденных ситуаций и тщательность проверок, а также сбор и управление информацией по инцидентам безопасности. Поэтому важно, чтобы организация планировала и управляла переходом к договорам аутсорсинга, и применяла соответствующий процесс менеджмента изменений и перезаключения/окончания действия договоров.

В договоре необходимо учитывать процедуры непрерывной обработки на случай, если третья сторона окажется неспособной поставлять свои услуги, для предотвращения какой-либо задержки по организации замены услуг.

В договорах с третьими сторонами могут участвовать также и другие стороны. Договоры, предоставляющие доступ третьим сторонам, должны содержать разрешение на привлечение других организаций, а также условия их доступа и участия.

Как правило, договоры разрабатываются, в первую очередь, организацией. Иногда договор может быть разработан и предложен организации третьей стороной. Организации необходимо обеспечивать уверенность в том, что требования третьей стороны, изложенные в предлагаемых договорах, не оказывают излишнего влияния на ее собственную безопасность.

7 Менеджмент активов

7.1 Ответственность за активы

Цель: Обеспечить соответствующую защиту активов организации.

Все активы должны учитываться и иметь назначенного владельца.

Необходимо определять владельцев всех активов, и следует определять ответственного за поддержку соответствующих мер и средств контроля и управления. Реализация определенных мер и средств контроля и управления при необходимости может быть делегирована владельцем, но владелец остается ответственным за надлежащую защиту активов.

7.1.1 Инвентаризация активов

Мера и средство контроля и управления

Все активы должны быть четко определены, должна составляться и поддерживаться опись всех важных активов.

Рекомендация по реализации

Организации следует идентифицировать все активы и документально оформлять значимость этих активов. В опись активов следует включить всю информацию, необходимую для восстановления после бедствия, в том числе тип актива, формат, местоположение, информацию о резервных копиях, информацию о лицензировании и ценности для бизнеса. Опись не должна без необходимости дублировать другие описи, но следует обеспечивать уверенность в том, что ее содержание выверено.

Кроме того, владение (см. 7.1.2) и классификация информации (см. 7.2) должны быть согласованы и документально оформлены в отношении каждого актива. Основываясь на важности актива, его ценности для бизнеса и его категории секретности, надлежит определить уровни защиты, соответствующие значимости активов (более подробную информацию о том, как оценивать активы, чтобы учесть их важность, можно найти в ИСО/МЭК 27005).

Дополнительная информация

Существует много типов активов, включающих:

a) информацию: базы данных и файлы данных, договоры и соглашения, системная документация, исследовательская информация, руководства пользователя, учебные материалы, процедуры эксплуатации или поддержки, планы непрерывности бизнеса, меры по переходу на аварийный режим, контрольные записи и архивированная информация;

b) программные активы: прикладные программные средства, системные программные средства, средства разработки и утилиты;

c) физические активы: компьютерное оборудование, средства связи, съемные носители информации и другое оборудование;

d) услуги: вычислительные услуги и услуги связи, основные поддерживающие услуги, например отопление, освещение, электроэнергия и кондиционирование воздуха;

e) персонал, его квалификация, навыки и опыт;

f) нематериальные ценности, например репутация и имидж организации.

Описи активов помогают обеспечивать уверенность в том, что активы организации эффективно защищены, данные описи могут также потребоваться для других целей, таких как обеспечение безопасности труда, страховые или финансовые (менеджмент активов) вопросы. Процесс инвентаризации активов — важное условие для менеджмента риска.

7.1.2 Владение активами

Мера и средство контроля и управления

Вся информация и активы, связанные со средствами обработки информации должны находиться во владении[1)] определенной части организации.

Рекомендация по реализации

Владелец актива должен нести ответственность за:

a) обеспечение уверенности в том, что информация и активы, связанные со средствами обработки информации, классифицированы соответствующим образом;

[1)] Термином «владелец» определяется физическое или юридическое лицо, которое наделено административной ответственностью за руководство изготовлением, разработкой, хранением, использованием и безопасностью активов. Термин «владелец» не означает, что данный человек фактически имеет право собственности на этот актив.

b) определение и периодический пересмотр ограничений и классификаций доступа, принимая в расчет применимые политики управления доступом.

Владение может распространяться на:

a) процесс бизнеса;

b) определенный набор деятельностей;

c) прикладные программы;

d) определенное множество данных.

Дополнительная информация

Повседневные задачи могут быть переданы, например должностному лицу, ежедневно работающему с активом, но ответственность сохраняется за владельцем.

В сложных информационных системах рекомендуется обозначить группы активов, действующих вместе, для обеспечения определенной функции, такой как «услуга». В данном случае владелец услуг является ответственным за поставку услуги и функционирование активов, которые обеспечивают данную услугу.

7.1.3 Приемлемое использование активов

Мера и средство контроля и управления

Следует определять, документально оформлять и реализовывать правила приемлемого использования информации и активов, связанных со средствами обработки информации.

Рекомендация по реализации

Всем служащим, подрядчикам и представителям третьей стороны рекомендуется следовать правилам приемлемого использования информации и активов, связанных со средствами обработки информации, включая:

a) правила использования электронной почты и Интернета (см. 10.8);

b) рекомендации по использованию мобильных устройств, особенно в отношении использования их за пределами помещений организации (см. 11.7.1).

Соответствующему управленческому персоналу должны быть предоставлены конкретные правила или рекомендации. Служащие, подрядчики и представители третьей стороны, использующие или имеющие доступ к активам организации, должны быть осведомлены о существующих ограничениях в отношении использования ими информации и активов организации, связанных со средствами обработки информации и ресурсами. Они должны нести ответственность за использование ими любых средств обработки информации, и любое использование таких средств осуществлять под свою ответственность.

7.2 Классификация информации

Цель: Обеспечить уверенность в защищенности информации на надлежащем уровне.

Информацию следует классифицировать, чтобы определить необходимость, приоритеты и предполагаемую степень защиты при обработке информации.

Информация имеет различные степени чувствительности и критичности. Некоторые элементы могут потребовать дополнительного уровня защиты или специальной обработки. Схему классификации информации следует использовать для определения соответствующего множества уровней защиты и установления потребности в принятии специальных мер обработки.

7.2.1 Рекомендации по классификации

Мера и средство контроля и управления

Информацию следует классифицировать, исходя из ее ценности, законодательных требований, чувствительности и критичности для организации.

Рекомендация по реализации

При классификации информации и связанных с ней защитных мер и средств контроля и управления необходимо учитывать требования бизнеса в отношении совместного использования или ограничения доступа к информации и последствия для бизнеса, связанные с такими требованиями.

Рекомендации по классификации должны включать руководящие указания по начальной классификации и последующей классификации по истечении времени в соответствии с некой предопределенной политикой управления доступом (см. 11.1.1).

В обязанности владельца актива (см. 7.1.2) входит классификация актива, ее периодический пересмотр и обеспечение уверенности в том, что она поддерживается на актуальном и соответствующем уровне. В отношении классификации следует учитывать эффект накопления, указанный в 10.7.2.

Предметом рассмотрения должно стать количество классификационных категорий и преимущества, получаемые от их использования. Чрезмерно сложные схемы могут стать обременительными и неоправданно дорогими для применения, или могут оказаться неосуществимыми. Следует проявлять осторож-

ность в интерпретации классификационных меток на документах из других организаций, так как одни и те же метки могут иметь различный смысл.

Дополнительная информация

Уровень защиты может оцениваться с помощью анализа конфиденциальности, целостности и доступности, а также каких-либо других требований в отношении рассматриваемой информации.

Информация часто перестает быть чувствительной или критической по истечении некоторого периода времени, например когда она делается общедоступной. Эти аспекты необходимо принимать во внимание, поскольку присвоение более высокой категории может привести к реализации ненужных мер и средств контроля и управления и, как следствие, к дополнительным расходам.

При назначении классификационных уровней, совместное рассмотрение документов с аналогичными требованиями безопасности может упростить задачу по классификации.

В общем, классификация информации — кратчайший путь для определения способа ее обработки и защиты.

7.2.2 Маркировка и обработка информации

Мера и средство контроля и управления

Соответствующий набор процедур маркировки и обработки информации следует разрабатывать и реализовывать в соответствии с системой классификации, принятой организацией.

Рекомендация по реализации

Необходимо, чтобы процедуры маркировки информации охватывали информационные активы, представленные как в физической, так и в электронной форме.

Выводимые из систем документы, содержащие информацию, которая классифицирована как чувствительная или критическая, должны содержать соответствующий маркировочный знак. Маркировка должна отражать классификацию согласно правилам, установленным в 7.2.1. Маркированными могут быть напечатанные отчеты, экранные отображения, носители информации (например ленты, диски, компакт-диски), электронные сообщения и пересылаемые файлы.

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

Договоры с другими организациями, включающие требования о совместном использовании информации, должны содержать процедуры определения классификации этой информации и интерпретации классификационных меток других организаций.

Дополнительная информация

Маркировка и безопасная обработка классифицированной информации является ключевым требованием для соглашений о совместном использовании информации. Физические метки являются наиболее распространенной формой маркировки. Однако некоторые информационные активы, например документы в электронной форме, не могут быть маркированы физически, и поэтому необходимо использовать электронные аналоги маркировки. Например на экране или дисплее может появиться уведомляющая метка. Там, где маркировка неосуществима, применяют другие средства обозначения классификации информации, например с помощью процедур или метаданных.

8 Безопасность, связанная с персоналом

8.1 Перед трудоустройством[1)]

Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и представители третьей стороны осознают свои обязанности и способны выполнять предусмотренные для них роли, и снизить риск хищения, мошенничества или нецелевого использования средств обработки информации.

Обязанности, связанные с обеспечением безопасности, следует оговаривать перед трудоустройством в соответствующих должностных инструкциях и условиями работы.

Необходима соответствующая проверка всех кандидатов на должность, подрядчиков и представителей третьей стороны, особенно если работа связана с секретностью.

[1)] Пояснение: Под словом «трудоустройство» здесь понимается охват всех следующих отличающихся друг от друга ситуаций: трудоустройство людей (временное или постоянное), указание должностных функций (ролей), изменение должностных функций, определение срока действия договоров и прекращение любой из этих договоренностей.

Сотрудники, подрядчики и представители третьей стороны, использующие средства обработки информации организации, должны подписывать соглашение в отношении их ролей и обязанностей в области безопасности.

8.1.1 Роли и обязанности

Мера и средство контроля и управления

Роли и обязанности в области безопасности сотрудников, подрядчиков и представителей третьей стороны необходимо определять и оформлять документально в соответствии с политикой информационной безопасности организации.

Рекомендация по реализации

Роли и обязанности в области безопасности должны включать в себя требования в отношении:

a) реализации и действия в соответствии с политиками информационной безопасности организации (см. 5.1);

b) защиты активов от несанкционированного доступа, разглашения сведений, модификации, разрушений или вмешательства;

c) выполнения определенных процессов или деятельности, связанных с безопасностью;

d) обеспечения уверенности в том, что на индивидуума возлагается ответственность за предпринимаемые действия;

e) информирования о событиях или потенциальных событиях, связанных с безопасностью, или других рисках безопасности для организации.

Роли и обязанности в области безопасности должны быть определены и доведены до претендентов на работу до их трудоустройства.

Дополнительная информация

Для документального оформления ролей и обязанностей в области безопасности могут использоваться должностные инструкции. Роли и обязанности в области безопасности лиц, поступивших на работу не через процесс трудоустройства, принятый в организации, а, например с помощью сторонней организации, должны быть также четко определены и доведены до сведения.

8.1.2 Предварительная проверка

Мера и средство контроля и управления

Тщательная проверка всех кандидатов на постоянную работу, подрядчиков и представителей третьей стороны должна проводиться согласно соответствующим законам, инструкциям и правилам этики, пропорционально требованиям бизнеса, классификации информации, к которой будет осуществляться доступ, и предполагаемым рискам.

Рекомендация по реализации

При проверке следует учитывать конфиденциальность, защиту персональных данных и (или) трудовое законодательство. Такая проверка должна включать следующие элементы:

a) наличие положительных рекомендаций, в частности, в отношении деловых и личных качеств претендента;

b) проверку (на предмет полноты и точности) биографии претендента;

c) подтверждение заявленного образования и профессиональной квалификации;

d) независимую проверку подлинности документов, удостоверяющих личность (паспорта или заменяющего его документа);

e) более детальную проверку, например кредитоспособности или на наличие судимости.

В случаях, когда новому сотруднику непосредственно после приема на работу или в дальнейшем предоставляется доступ к средствам обработки информации, в частности, обрабатывающим чувствительную информацию, например финансовую или секретную информацию, организации следует проводить дополнительную, более детальную проверку.

Процедуры должны определять критерии и ограничения процесса проверки, например кто имеет право проводить проверку сотрудников, каким образом, когда и с какой целью проводится эта проверка.

Предварительную проверку также следует проводить для подрядчиков и представителей третьей стороны. В тех случаях, когда подрядчики предоставляются через кадровое агентство, контракт с агентством должен четко определять обязанности агентства по предварительной проверке претендентов и процедурам уведомления, которым оно должно следовать, если предварительная проверка не была закончена, или если ее результаты дают основания для сомнения. Как бы то ни было, в договорах с третьей стороной (см. 6.2.3) должны четко определяться все обязанности и процедуры уведомления, необходимые для предварительной проверки.

Информацию обо всех рассматриваемых кандидатах, претендующих на занятие должностей в организации, следует собирать и обрабатывать согласно законодательству, действующему в соответствующей юрисдикции. В зависимости от действующего законодательства, данные кандидаты должны быть предварительно проинформированы о деятельности, связанной с предварительной проверкой.

8.1.3 Условия занятости

Мера и средство контроля и управления

В рамках своих договорных обязательств, сотрудники, подрядчики и представители третьей стороны должны согласовать и подписать условия своего трудового договора, устанавливающего их ответственность и ответственность организации в отношении информационной безопасности.

Рекомендация по реализации

Условия занятости должны отражать политику безопасности организации и кроме того разъяснять и констатировать:

a) что все сотрудники, подрядчики и представители третьей стороны, имеющие доступ к чувствительной информации, должны подписывать соглашение о конфиденциальности или неразглашении прежде, чем им будет предоставлен доступ к средствам обработки информации;

b) правовую ответственность и права сотрудников, подрядчиков и любых других клиентов, например в части законов об авторском праве или законодательства о защите персональных данных (см. 15.1.1 и 15.1.2);

c) обязанности в отношении классификации информации и менеджмента активов организации, связанных с информационными системами и услугами, выполняются сотрудником, подрядчиком или представителем третьей стороны (см. 7.2.1 и 10.7.3);

d) ответственность сотрудника, подрядчика или представителя третьей стороны за обработку информации, получаемой от других фирм и сторонних организаций;

e) ответственность организации за обработку персональной информации, включая персональную информацию, полученную в результате или в процессе работы в организации (см. 15.1.4);

f) ответственность, распространяющуюся также и на работу вне помещений организации и в нерабочее время, например в случае исполнения работы на дому (см. 9.2.5 и 11.7.1);

g) действия, которые должны быть предприняты в случае, если сотрудник, подрядчик или представитель третьей стороны игнорирует требования безопасности организации (см. 8.2.3).

Организация должна обеспечивать уверенность в том, что сотрудники, подрядчики и представители третьей стороны согласны с условиями, касающимися информационной безопасности и соответствующими типу и объему доступа, который они будут иметь к активам организации, связанным с информационными системами и услугами.

При необходимости ответственность, возлагаемая на сотрудника по условиям занятости, должна сохраняться сотрудником в течение определенного периода времени и после окончания работы в организации (см. 8.3).

Дополнительная информация

Может быть использован кодекс поведения для распространения информации, касающейся обязанностей сотрудников, подрядчиков или представителей третьей стороны в отношении конфиденциальности, защиты информации, правил этики, соответствующего использования оборудования и средств организации, а также порядка деятельности. Подрядчик или представители третьей стороны могут быть связаны со сторонней организацией, с которой, в свою очередь, может потребоваться заключить договорные соглашения от имени лица, подписавшего договор.

8.2 В течение занятости

Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и представители третьей стороны осведомлены об угрозах и проблемах, связанных с информационной безопасностью, о мере их ответственности и обязательствах, а также оснащены всем необходимым для поддержки политики безопасности организации, что снижает риск человеческого фактора.

Следует определять обязанности руководства, чтобы обеспечить уверенность в том, что безопасность обеспечивается на протяжении всего времени занятости сотрудника в организации.

Адекватный уровень осведомленности, обучения и тренинг процедурам безопасности и правильному использованию средств обработки информации должен быть обеспечен всем сотрудникам, подрядчикам и представителям третьей стороны, чтобы свести к минимуму возможные риски безопасности. Должен быть установлен формальный дисциплинарный процесс для рассмотрения нарушений безопасности.

8.2.1 Обязанности руководства

Мера и средство контроля и управления

Руководство организации должно требовать, чтобы сотрудники, подрядчики и представители третьей стороны обеспечивали безопасность в соответствии с установленными политиками и процедурами организации.

Рекомендация по реализации

Руководство обязано обеспечить уверенность в том, что сотрудники, подрядчики и представители третьей стороны:

a) были проинформированы о своих ролях и обязанностях в области информационной безопасности прежде, чем им был предоставлен доступ к чувствительной информации или информационным системам;

b) обеспечены рекомендациями по формулированию их предполагаемых ролей в отношении безопасности в рамках организации;

c) заинтересованы следовать политикам безопасности организации;

d) достигают уровня осведомленности в отношении безопасности, соответствующего их ролям и обязанностям в организации (см. 8.2.2);

e) следуют условиям занятости, которые включают политику информационной безопасности организации и соответствующие методы работы;

f) продолжают поддерживать соответствующие навыки и квалификацию.

Дополнительная информация

Если сотрудники, подрядчики и представители третьей стороны не были осведомлены о своих обязанностях в отношении безопасности, они могут причинить значительный ущерб организации. Заинтересованный персонал, вероятно, будет более надежным и вызовет меньше инцидентов информационной безопасности.

Неэффективный менеджмент может являться причиной того, что персонал будет чувствовать себя недооцененным, что в дальнейшем может иметь негативные последствия для организации. Например неэффективный менеджмент может привести к игнорированию безопасности или возможному нецелевому использованию активов организации.

8.2.2 Осведомленность, обучение и тренинг в области информационной безопасности

Мера и средство контроля и управления

Все сотрудники организации и, где необходимо, подрядчики и представители третьей стороны, должны пройти соответствующее обучение и получать на регулярной основе обновленные варианты политик и процедур, принятых в организации и необходимых для выполнения их рабочих функций.

Рекомендация по реализации

Обучение, обеспечивающее осведомленность, следует начинать с формального вводного процесса, предназначенного для ознакомления с политиками и ожиданиями организации в области безопасности прежде, чем будет предоставлен доступ к информации или услугам.

Постоянное обучение должно охватывать требования безопасности, правовую ответственность, управление бизнесом, а также обучение правильному использованию средств обработки информации, например процедуре начала сеанса, использованию пакетов программ и информации о дисциплинарном процессе (см. 8.2.3).

Дополнительная информация

Деятельность, связанная с обеспечением осведомленности, обучения и тренинга в отношении безопасности должна быть адекватной и соответствовать роли, обязанностям и квалификации лица, и должна включать информацию об известных угрозах, о контактном лице для получения дополнительной консультации по безопасности, а также о соответствующих каналах для сообщения об инцидентах информационной безопасности (см. 13.1).

Обучение с целью повышения осведомленности направлено на то, чтобы дать возможность отдельным лицам распознавать проблемы и инциденты информационной безопасности, и реагировать в соответствии с потребностями их рабочей функции.

8.2.3 Дисциплинарный процесс

Мера и средство контроля и управления

Должен существовать формальный дисциплинарный процесс, применяемый в отношении сотрудников, совершивших нарушение безопасности.

Рекомендация по реализации

Не следует начинать дисциплинарный процесс, не получив предварительного подтверждения того, что нарушение безопасности произошло (см. 13.2.3).

Формальный дисциплинарный процесс призван обеспечить уверенность в корректном и справедливом рассмотрении дел сотрудников, подозреваемых в совершении нарушений безопасности. Формальный дисциплинарный процесс следует обеспечивать для дифференцированного реагирования, учитывающего такие факторы, как тип и тяжесть нарушения и его негативное влияние на бизнес, совершено ли нарушение впервые или повторно, получил ли нарушитель должную подготовку, соответствующее законодательство, договоры в сфере бизнеса и другие факторы, если в этом есть необходимость. В серьезных случаях неправомерного поведения процесс должен обеспечивать возможность безотлагательного аннулирования обязанностей, прав доступа и привилегий сотрудника и, при необходимости, немедленного удаления его из информационного процесса.

Дополнительная информация

Дисциплинарный процесс следует также использовать как сдерживающее средство для предотвращения совершения сотрудниками, подрядчиками и представителями третьей стороны нарушений политик и процедур безопасности, принятых в организации, и каких-либо других нарушений безопасности.

8.3 Прекращение или смена занятости

Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и представители третьей стороны покидают организацию или меняют занятость должным образом.

Администрация обязана обеспечить уверенность в том, что при увольнении сотрудников, подрядчиков и представителей третьей стороны из организации, осуществляется возврат всего оборудования, а также выполняется аннулирование всех прав доступа.

Изменения обязанностей и занятости, равно как и прекращение соответствующей обязанности и занятости в рамках организации должно управляться в соответствии с данным подразделом, а любая новая занятость должна управляться, как описано в 8.1.

8.3.1 Прекращение обязанностей

Мера и средство контроля и управления

Обязанности в отношении прекращения занятости или смены занятости должны быть четко определены и установлены.

Рекомендация по реализации

Информирование о прекращении обязанностей должно включать в себя актуальные требования безопасности и правовую ответственность, и, при необходимости, обязанности, содержащиеся в соглашении о конфиденциальности (см. 6.1.5), а также условия занятости (см. 8.1.3), продолжающие действовать в течение определенного периода времени после прекращения занятости сотрудников, подрядчиков или представителей третьей стороны.

Ответственность и служебные обязанности, продолжающие оставаться действительными после прекращения занятости, должны содержаться в договорах с сотрудниками, подрядчиками или представителями третьей стороны.

Изменения обязанности и занятости должны управляться также как и прекращение соответствующей обязанности или занятости, а управление новой обязанностью или занятостью должно осуществляться так, как это описано в 8.1.

Дополнительная информация

Отдел кадров, как правило, отвечает за общий процесс прекращения занятости и действует совместно с руководителем увольняемого лица, чтобы обеспечить управление аспектами безопасности значимых процедур. В отношении подрядчика данный процесс может быть осуществлен агентством, несущим ответственность за подрядчика, а в отношении представителя третьей стороны — его организацией.

Сотрудников, клиентов, подрядчиков или представителей третьей стороны необходимо информировать об изменениях кадрового состава и действующих договоренностей.

8.3.2 Возврат активов

Мера и средство контроля и управления

Все сотрудники, подрядчики и представители третьей стороны обязаны вернуть организации все активы, находящиеся в их пользовании, при прекращении их занятости, договора или соглашения.

Рекомендация по реализации

Процесс прекращения занятости должен быть формализован таким образом, чтобы включать в себя возврат всего ранее выданного программного обеспечения, корпоративных документов и оборудования. Необходимо возвращать также другие активы организации, например мобильную вычислительную техни-

ку, кредитные карты, карты доступа, программное обеспечение, руководства и информацию, хранящуюся на электронных носителях.

В тех случаях, когда сотрудник, подрядчик или представитель третьей стороны покупает оборудование организации или использует свое собственное оборудование, необходимо следовать процедурам, обеспечивающим уверенность в том, что вся значимая информация была передана организации и удалена из оборудования безопасным образом (см. 10.7.1).

В случаях, когда сотрудник, подрядчик или представитель третьей стороны располагает знаниями, важными для продолжающихся работ, такую информацию следует оформлять документально и передавать организации.

8.3.3 Аннулирование прав доступа

Мера и средство контроля и управления

Права доступа всех служащих, подрядчиков и представителей третьей стороны к информации и средствам обработки информации должны быть аннулированы при прекращении занятости, договора или соглашения, или скорректированы при смене занятости.

Рекомендация по реализации

При прекращении занятости, права доступа к активам, связанным с информационными системами, и услугам необходимо пересматривать. Это позволит определять, нужно ли аннулировать права доступа. Смена занятости должна сопровождаться аннулированием всех прав доступа, которые не санкционированы для новой занятости. Права доступа, которые должны быть аннулированы или адаптированы, касаются физического и логического доступа, ключей, идентификационных карт, средств обработки информации (см. также 11.2.4), подписок и удаления из любой документации, в которой они идентифицируются как фактические сотрудники организации. Если увольняемый сотрудник, подрядчик или представитель третьей стороны знал пароли к учетным записям, остающимся активными, то эти пароли должны быть изменены после прекращения занятости, договора или соглашения, или при смене занятости.

Права доступа к информационным активам и средствам обработки информации следует уменьшать или аннулировать до прекращения занятости или смены места занятости, в зависимости от оценки факторов риска, например:

a) было ли прекращение занятости или смена места занятости инициированы сотрудником, подрядчиком или представителем третьей стороны, или руководством, и причина прекращения занятости;

b) текущие обязанности сотрудника, подрядчика или любого другого представителя;

c) значимость активов, доступных в настоящий момент.

Дополнительная информация

При определенных обстоятельствах права доступа могут распределяться на основе доступности для большего количества людей, чем только для увольняемого сотрудника, подрядчика или представителя третьей стороны, например групповые идентификаторы. При таких обстоятельствах увольняемых лиц следует исключать из любых списков группового доступа, и следует предпринимать меры, рекомендующие всем другим связанным с доступом сотрудникам, подрядчикам и представителям третьей стороны не осуществлять совместно с увольняемым лицом использования этой информации.

В случаях, когда прекращение занятости инициируется руководством, рассерженные сотрудники, подрядчики или представители третьей стороны могут преднамеренно разрушать информацию или повреждать средства обработки информации. В случаях ухода в отставку, некоторые лица склонны собирать информацию для будущего использования.

9 Физическая безопасность и защита от воздействий окружающей среды

9.1 Зоны безопасности

Цель: Предотвращать неавторизованный физический доступ, повреждение и воздействие в отношении помещений и информации организации.

Средства обработки критической или чувствительной информации необходимо размещать в зонах безопасности, обозначенных определенным периметром безопасности, обладающим соответствующими защитными барьерами и средствами, контролирующими вход. Эти зоны должны быть физически защищены от неавторизованного доступа, повреждения и воздействия.

Уровень защищенности должен быть соразмерен выявленным рискам.

9.1.1 Периметр зоны безопасности

Мера и средство контроля и управления

Для защиты зон, которые содержат информацию и средства обработки информации, следует использовать периметры безопасности (барьеры, например стены, управляемые картами доступа ворота или турникеты, управляемые человеком).

Рекомендация по реализации

В отношении физических периметров безопасности рекомендуется рассматривать и реализовывать, при необходимости, следующие рекомендации:

a) периметры безопасности должны быть четко определены, а размещение и надежность каждого из периметров должны зависеть от требований безопасности активов, находящихся в пределах периметра, и от результатов оценки риска;

b) периметры здания или помещений, где расположены средства обработки информации, должны быть физически прочными (т. е. не должно быть никаких промежутков в периметре или мест, через которые можно было бы легко проникнуть); внешние стены помещений должны иметь твердую конструкцию, а все внешние двери должны быть соответствующим образом защищены от неавторизованного доступа, например оснащены шлагбаумом, сигнализацией, замками т. п.; двери и окна помещений в отсутствие сотрудников должны быть заперты, и внешняя защита должна быть предусмотрена для окон, особенно если они находятся на уровне земли;

c) должна быть выделена и укомплектована персоналом зона регистрации посетителей, или должны существовать другие меры для контроля физического доступа в помещения или здания; доступ в помещения и здания должен предоставляться только авторизованному персоналу;

d) где необходимо, должны быть построены физические барьеры, предотвращающие неавторизованный физический доступ и загрязнение окружающей среды;

e) все аварийные выходы на случай пожара в периметре безопасности должны быть оборудованы аварийной сигнализацией, должны подвергаться мониторингу и тестированию вместе со стенами, чтобы создать требуемый уровень устойчивости в соответствии с применимыми региональными, национальными и международными стандартами; они должны эксплуатироваться в соответствии с местной системой противопожарных правил безотказным образом;

f) следует устанавливать необходимые системы обнаружения вторжения, соответствующие национальным, региональным или международным стандартам, и регулярно тестировать их на предмет охвата всех внешних дверей и доступных окон, свободные помещения необходимо ставить на сигнализацию; аналогично следует оборудовать и другие зоны, например серверную комнату или помещение, где расположены средства коммуникаций;

g) необходимо физически изолировать средства обработки информации, контролируемые организацией, от средств, контролируемых сторонними организациями.

Дополнительная информация

Физическая защита может быть обеспечена созданием одного или нескольких физических барьеров вокруг помещений и средств обработки информации организации. Использование нескольких барьеров дает дополнительную защиту, и повреждение одного барьера не означает немедленного нарушения безопасности.

Зоной безопасности может быть запираемый офис или несколько помещений внутри физического барьера безопасности. Между зонами с различными требованиями безопасности, находящимися внутри периметра безопасности, могут потребоваться дополнительные барьеры и периметры для контроля физического доступа.

В отношении безопасности физического доступа особое внимание следует обращать на здания, в которых размещено несколько организаций.

9.1.2 Меры и средства контроля и управления физическим входом

Мера и средство контроля и управления

Зоны безопасности необходимо защищать с помощью соответствующих мер и средств контроля и управления входа, чтобы обеспечить уверенность в том, что доступ разрешен только авторизованному персоналу.

Рекомендация по реализации

Следует принимать во внимание следующие рекомендации:

a) дату и время входа и выхода посетителей следует регистрировать, и всех посетителей необходимо сопровождать, или они должны обладать соответствующим допуском; доступ следует предоставлять

только для выполнения определенных авторизованных задач, а также необходимо инструктировать посетителей на предмет требований безопасности, и действий в случае аварийных ситуаций;

b) доступ к зонам, где обрабатывается или хранится чувствительная информация, должен контролироваться и предоставляться только авторизованным лицам; следует использовать средства аутентификации, например контрольную карту доступа с персональным идентификационным номером (ПИН) для авторизации и проверки всех видов доступа; необходимо вести защищенные контрольные записи регистрации доступа;

c) необходимо требовать, чтобы все сотрудники, подрядчики и представители третьей стороны носили ту или иную форму видимого идентификатора и незамедлительно уведомляли сотрудников службы безопасности о замеченных несопровождаемых посетителях и лицах, не носящих видимого идентификатора;

d) доступ в зоны безопасности или к средствам обработки чувствительной информации персоналу вспомогательных служб третьей стороны следует предоставлять только при необходимости; такой доступ должен быть санкционирован и сопровождаться соответствующим контролем;

e) права доступа в зоны безопасности следует регулярно анализировать, пересматривать, и аннулировать при необходимости (см. 8.3.3).

9.1.3 Безопасность зданий, производственных помещений и оборудования

Мера и средство контроля и управления

Необходимо разработать и реализовать физическую защиту зданий, производственных помещений и оборудования.

Рекомендация по реализации

В отношении защиты зданий, производственных помещений и оборудования необходимо учитывать следующие рекомендации:

a) следует принимать в расчет соответствующие правила и стандарты, касающиеся охраны здоровья и безопасности труда;

b) основное оборудование должно быть расположено в местах, где ограничен доступ посторонним лицам;

c) здания, где это применимо, должны давать минимальную информацию относительно их предназначения, не должны иметь явных признаков снаружи или внутри здания, позволяющих установить наличие деятельности по обработке информации;

d) справочники и внутренние телефонные книги, указывающие на местоположение средств обработки чувствительной информации, не должны быть легкодоступными для посторонних лиц.

9.1.4 Защита от внешних угроз и угроз со стороны окружающей среды

Мера и средство контроля и управления

Необходимо разработать и реализовать физическую защиту от нанесения ущерба, который может явиться результатом пожара, наводнения, землетрясения, взрыва, общественных беспорядков и других форм природных или антропогенных бедствий.

Рекомендация по реализации

Необходимо предусмотреть любые угрозы безопасности, исходящие от соседних помещений, например пожар в соседнем здании, воду, текущую с крыши или затопившую этажи, находящиеся ниже уровня земли, или взрыв на улице.

Для предотвращения ущерба от пожара, наводнения, землетрясения, взрыва, общественных беспорядков и других форм природных или антропогенных бедствий, следует учитывать следующие рекомендации:

a) обеспечить надежное хранение опасных или горючих материалов на достаточном расстоянии от охраняемой зоны; большие запасы, например бумаги для печатающих устройств, не следует хранить в пределах зоны безопасности;

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

c) следует обеспечить и соответствующим образом разместить необходимые средства пожаротушения.

9.1.5 Работа в зонах безопасности

Мера и средство контроля и управления

Необходимо разработать и реализовать физическую защиту и рекомендации по работе в зонах безопасности.

Рекомендация по реализации

Необходимо рассмотреть следующие рекомендации:

a) о существовании зоны безопасности и проводимых там работах персонал должен быть осведомлен по «принципу необходимого знания»;

b) из соображений безопасности и предотвращения возможности злонамеренных действий в зонах безопасности необходимо избегать выполнения 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- и другого записывающего оборудования, например камер, имеющихся в мобильных устройствах, должно быть запрещено, если только на это не получено специальное разрешение.

Меры и средства контроля и управления, связанные с работой в зонах безопасности, включают в себя меры и средства контроля и управления, применяемые в отношении сотрудников, подрядчиков и представителей третьей стороны, работающих в зоне безопасности, а также в отношении других видов деятельности третьей стороны, выполняемых там.

9.1.6 Зоны общего доступа, приемки и отгрузки

Мера и средство контроля и управления

Места доступа, например зоны приемки и отгрузки, и другие места, где неавторизованные лица могут проникнуть в помещения, должны находиться под контролем и, по возможности, должны быть изолированы от средств обработки информации, во избежание неавторизованного доступа.

Рекомендация по реализации

Необходимо рассмотреть следующие рекомендации:

a) доступ к зоне приемки и отгрузки с внешней стороны здания должен быть разрешен только определенному и авторизованному персоналу;

b) зона приемки и отгрузки должна быть организована так, чтобы поступающие материальные ценности могли быть разгружены без предоставления персоналу поставщика доступа к другим частям здания;

c) должна быть обеспечена безопасность внешних дверей зоны приемки и отгрузки в то время, когда внутренние двери открыты;

d) поступающие материальные ценности должны быть проверены на предмет потенциальных угроз (см. перечисление d) 9.2.1) прежде, чем они будут перемещены из зоны приемки и отгрузки к месту использования;

e) при поступлении материальные ценности должны регистрироваться в соответствии с процедурами менеджмента активов (см. 7.1.1);

f) там, где возможно, ввозимые и вывозимые грузы должны быть физически разделены.

9.2 Безопасность оборудования

Цель: Предотвращать потерю, повреждение, кражу или компрометацию активов и прерывание деятельности организации.

Оборудование необходимо защищать от физических угроз и воздействия окружающей среды.

Обеспечение безопасности оборудования (включая используемое вне организации и выносимое имущество) необходимо для уменьшения риска неавторизованного доступа к информации и защиты ее от потери или повреждения. При этом следует учесть размещение и утилизацию оборудования. Могут потребоваться специальные меры и средства контроля и управления для защиты от физических угроз, а также для защиты инфраструктуры поддерживающих услуг, например системы электропитания и кабельной разводки.

9.2.1 Размещение и защита оборудования

Мера и средство контроля и управления

Оборудование должно быть размещено и защищено так, чтобы уменьшить риски от угроз окружающей среды и возможности неавторизованного доступа.

Рекомендация по реализации

Необходимо рассмотреть следующие рекомендации по защите оборудования:

a) оборудование следует размещать таким образом, чтобы свести к минимуму излишний доступ в рабочие зоны;

b) средства обработки информации, обрабатывающие чувствительные данные, следует размещать и ограничивать угол обзора таким образом, чтобы уменьшить риск просмотра информации неавторизованными лицами во время их использования, а средства хранения информации следует защищать от неавторизованного доступа;

c) отдельные элементы оборудования, требующие специальной защиты, следует изолировать для снижения общего уровня требуемой защиты;

d) меры и средства контроля и управления должны быть внедрены таким образом, чтобы свести к минимуму риск потенциальных физических угроз (воровство, пожар, взрывы, задымление, затопление или неисправность водоснабжения, пыль, вибрация, химическое воздействие, помехи в электроснабжении, помехи в работе линий связи, электромагнитное излучение и вандализм);

e) необходимо устанавливать правила в отношении приема пищи, питья и курения вблизи средств обработки информации;

f) следует проводить мониторинг состояния окружающей среды по выявлению условий, например температуры и влажности, которые могли бы оказать неблагоприятное влияние на функционирование средств обработки информации;

g) на всех зданиях должна быть установлена защита от молнии, а фильтры защиты от молнии должны быть установлены на входе всех линий электропередачи и линий коммуникации;

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

i) оборудование, обрабатывающее чувствительную информацию, должно быть защищено, чтобы свести к минимуму риск утечки информации вследствие излучения.

9.2.2 Поддерживающие услуги

Мера и средство контроля и управления

Оборудование необходимо защищать от перебоев подачи электроэнергии и других сбоев, связанных с перебоями в обеспечении поддерживающих услуг.

Рекомендация по реализации

Все поддерживающие услуги, например электроснабжение, водоснабжение, канализация, отопление/вентиляция и кондиционирование воздуха, должны быть адекватными для поддерживаемых ими систем. Объекты поддерживающих услуг необходимо регулярно проверять и тестировать для обеспечения уверенности в их должном функционировании и уменьшения любого риска, связанного с их неисправной работой или отказом. Необходимо обеспечить надлежащую подачу электропитания, соответствующую спецификациям производителя оборудования.

Оборудование, поддерживающее важнейшие процессы бизнеса, рекомендуется подключать через источники бесперебойного электропитания (ИБП), чтобы обеспечить его безопасное выключение и (или) непрерывное функционирование. В планах обеспечения непрерывности электроснабжения следует предусмотреть действия на случай отказа ИБП. Резервный генератор следует использовать, когда функционирование оборудования необходимо обеспечить во время длительного отказа подачи электроэнергии. Для обеспечения работы генератора в течение длительного времени необходимо обеспечить соответствующую поставку топлива. Оборудование ИБП и генераторы должны регулярно проверяться, чтобы обеспечить уверенность в наличии адекватной производительности, а также тестироваться в соответствии с рекомендациями производителя. Кроме того, следует обращать внимание на использование нескольких источников питания или, если организация большая, отдельной электроподстанции.

Аварийные выключатели электропитания необходимо расположить около запасных выходов помещений, в которых находится оборудование, чтобы ускорить отключение электропитания в критических ситуациях. Необходимо обеспечить работу аварийного освещения на случай отказа электропитания, потребляемого от сети.

Водоснабжение должно быть стабильным и адекватным для обеспечения кондиционирования воздуха, обеспечения работы устройств увлажнения и систем пожаротушения (там, где они используются). Неисправности в работе системы водоснабжения могут привести к повреждению оборудования или могут препятствовать эффективной работе системы пожаротушения. Следует оценивать необходимость установки системы сигнализации для обнаружения неправильного функционирования объектов поддерживающих услуг.

Связь телекоммуникационного оборудования с оборудованием провайдера услуг должна осуществляться, по меньшей мере, по двум различным маршрутам, чтобы предотвратить отказ в одном из соединительных маршрутов, который может сделать услугу по передаче речи невозможной. Услуги по передаче речи должны быть адекватными, чтобы удовлетворять местным законодательным требованиям в отношении аварийной связи.

Дополнительная информация

Вариантом достижения непрерывности электропитания будет наличие нескольких источников питания, что позволит избежать единой точки отказа в электропитании.

9.2.3 Безопасность кабельной сети

Мера и средство контроля и управления

Силовые и телекоммуникационные кабельные сети, по которым передаются данные или поддерживающие информационные услуги, необходимо защищать от перехвата информации или разрушения.

Рекомендация по реализации

В отношении безопасности кабельной сети следует рассмотреть следующие рекомендации:

a) силовые и телекоммуникационные линии, связанные со средством обработки информации, должны, по возможности, располагаться под землей или иметь адекватную альтернативную защиту;

b) сетевой кабель должен быть защищен от неавторизованных подключений или повреждения, например посредством использования специального кожуха или выбора маршрутов прокладки кабеля в обход общедоступных участков;

c) силовые кабели должны быть отделены от коммуникационных, чтобы предотвращать помехи;

d) следует использовать кабель и оборудование с четкой маркировкой, чтобы свести к минимуму эксплуатационные ошибки, например случайного внесения исправлений при ремонте сетевых кабелей;

e) для уменьшения вероятности ошибок следует использовать документально оформленный перечень исправлений;

f) дополнительные меры и средства контроля и управления для чувствительных или критических систем включают:

1) использование армированного кабельного канала, а также закрытых помещений или шкафов в контрольных и конечных точках;

2) использование дублирующих маршрутов прокладки кабеля и (или) альтернативных способов передачи, обеспечивающих соответствующую безопасность;

3) использование оптико-волоконных линий связи;

4) использование электромагнитного экранирования для защиты кабелей;

5) проведение технических осмотров и физических проверок подключения неавторизованных устройств к кабельной сети;

6) управляемый доступ к коммутационным панелям и электрощитовым.

9.2.4 Техническое обслуживание оборудования

Мера и средство контроля и управления

Должно проводиться надлежащее техническое обслуживание оборудования для обеспечения его непрерывной доступности и целостности.

Рекомендация по реализации

В отношении технического обслуживания оборудования следует рассмотреть следующие рекомендации:

a) оборудование должно обслуживаться в соответствии с рекомендуемыми поставщиком периодичностью и спецификациями;

b) техническое обслуживание и ремонт оборудования должны проводиться только авторизованным персоналом;

c) следует хранить записи обо всех предполагаемых или фактических неисправностях и всех видах профилактического обслуживания;

d) если запланировано техническое обслуживание оборудования, следует принимать соответствующие меры и средства контроля и управления, при этом необходимо учитывать, будет ли техническое обслуживание проводиться персоналом организации или за ее пределами; при необходимости, чувствительная информация из оборудования должна быть удалена, или специалисты по техническому обслуживанию и ремонту должны иметь соответствующий допуск;

e) должны соблюдаться все требования, устанавливаемые полисами страхования.

9.2.5 Безопасность оборудования вне помещений организации

Мера и средство контроля и управления

При обеспечении безопасности оборудования, используемого вне места его постоянной эксплуатации, следует учитывать различные риски, связанные с работой вне помещений организации.

Рекомендация по реализации

Независимо от права собственности использование оборудования для обработки информации вне помещений организации должно быть санкционировано руководством.

Следующие рекомендации необходимо учитывать в отношении защиты оборудования, используемого вне помещений организации:

a) оборудование и носители информации, взятые из помещений организации, не следует оставлять без присмотра в общедоступных местах; во время поездок портативные компьютеры нужно перевозить как ручную кладь и по возможности маскировать;

b) необходимо соблюдать инструкции изготовителей по защите оборудования, например по защите от воздействия сильных электромагнитных полей;

c) для работы на дому следует определить соответствующие меры и средства контроля и управления, исходя из оценки рисков, например использование запираемых шкафов для хранения документов, соблюдение политики «чистого стола», управление доступом к компьютерам и связь с офисом по защищенным сетям (см. также ИСО/МЭК 18028 «Сетевая Безопасность»);

d) с целью защиты оборудования, используемого вне помещений организации, должно проводиться адекватное страхование, покрывающее указанные риски.

Риски безопасности, например связанные с повреждением, воровством и подслушиванием, могут значительно отличаться для различных объектов и должны учитываться при определении наиболее подходящих мер и средств контроля и управления.

Дополнительная информация

Под оборудованием, используемым для обработки и хранения информации, понимаются все типы персональных компьютеров, электронных записных книжек, мобильных телефонов, смарт-карт, а также бумага или другие виды носителей информации, которые применяются для работы на дому или транспортируются за пределы обычных рабочих помещений.

Более подробную информацию о других аспектах защиты переносного оборудования можно найти в 11.7.1.

9.2.6 Безопасная утилизация или повторное использование оборудования

Мера и средство контроля и управления

Все компоненты оборудования, содержащие носители данных, следует проверять с целью обеспечения уверенности в том, что любые чувствительные данные и лицензионное программное обеспечение были удалены или перезаписаны безопасным образом до их утилизации.

Рекомендация по реализации

Носители данных, содержащие чувствительную информацию, необходимо физически уничтожать, или информацию необходимо разрушить, удалить или перезаписать способами, делающими исходную информации невосстановимой, а не использовать стандартные функции удаления и форматирования.

Дополнительная информация

Поврежденные устройства, содержащие чувствительные данные, могут потребовать проведения оценки рисков с целью определения элементов, которые должны быть физически разрушены, направлены на ремонт или игнорированы.

Информация может быть скомпрометирована вследствие небрежной утилизации или повторного использования оборудования (см. 10.7.2).

9.2.7 Перемещение имущества

Мера и средство контроля и управления

Оборудование, информацию или программное обеспечение можно использовать вне помещений организации только при наличии соответствующего разрешения.

Рекомендация по реализации

Необходимо учитывать следующие рекомендации:

a) оборудование, информацию или программное обеспечение можно использовать вне помещений организации только при наличии соответствующего разрешения;

b) сотрудники, подрядчики и представители третьей стороны, имеющие право разрешать перемещение активов за пределы места эксплуатации, должны быть четко определены;

c) сроки перемещения оборудования должны быть установлены и проверены на соответствие при возврате;

d) там, где необходимо и уместно, оборудование следует регистрировать при перемещении из помещений организации и при возврате.

Дополнительная информация

Выборочные проверки, проводимые для обнаружения неавторизованного перемещения имущества, также могут проводиться для обнаружения неавторизованных устройств регистрации, оружия и т. д.,

и предотвращения их вноса в помещения организации. Такие выборочные проверки необходимо выполнять согласно соответствующим законам и инструкциям. Сотрудники должны быть осведомлены о проведении выборочных проверок, а проверки должны проводиться только с разрешения соответствующего правовым и нормативным требованиям.

10 Менеджмент коммуникаций и работ

10.1 Эксплуатационные процедуры и обязанности

Цель: Обеспечить уверенность в надлежащем и безопасном функционировании средств обработки информации.

Должны быть установлены обязанности и процедуры в отношении управления и эксплуатации всех средств обработки информации, включая также разработку соответствующих эксплуатационных процедур.

С целью сведения к минимуму риска неправильного использования систем вследствие небрежности или злого умысла, следует, по возможности, реализовать принцип разграничения обязанностей.

10.1.1 Документальное оформление эксплуатационных процедур

Мера и средство контроля и управления

Эксплуатационные процедуры следует документально оформлять, соблюдать и делать доступными для всех нуждающихся в них пользователей.

Рекомендация по реализации

Документально оформленные процедуры должны быть подготовлены для действий системы, связанных со средствами обработки информации и связи, таких как процедуры запуска и завершения работы компьютеров (серверов), процедуры резервирования, текущего обслуживания и ремонта оборудования, обращения с носителями информации, управление работой в машинном зале и работы с почтой, а также процедуры обеспечения безопасности.

Данные процедуры должны содержать детальные инструкции по выполнению каждой работы, включая:

a) обработку и управление информацией;

b) резервирование (см. 10.5);

c) требования в отношении графика работ, включая взаимозависимости между системами, время начала самого ранней работы и время завершения самой последней работы;

d) инструкции по обработке ошибок или других исключительных ситуаций, которые могли бы возникнуть в процессе выполнения работы, включая ограничения на использование системных утилит (см. 11.5.4);

e) необходимые контакты на случай неожиданных эксплуатационных или технических проблем;

f) специальные инструкции по управлению выводом данных и обращению с носителями информации, например использование специальной бумаги для печатающих устройств или управление выводом конфиденциальных данных, включая процедуры по безопасной утилизации выходных данных в случае сбоев в работе (см. 10.7.2 и 10.7.3);

g) перезапуск системы и соответствующие процедуры восстановления на случай системных сбоев;

h) управление информацией, содержащейся в контрольных записях и системных журналах (см. 10.10).

Эксплуатационные процедуры и документально оформленные процедуры действий системы должны рассматриваться как официальные документы, а изменения в них должны санкционироваться руководством. Если технически возможно, менеджмент информационных систем необходимо осуществлять единообразно, используя одни и те же процедуры, инструментальные средства и утилиты.

10.1.2 Управление изменениями

Мера и средство контроля и управления

Изменения в конфигурации средств обработки информации и системах должны контролироваться.

Рекомендация по реализации

Эксплуатируемые системы и прикладное программное обеспечение должны быть предметом строгого контроля управления изменениями.

В частности, необходимо рассмотреть следующие аспекты:

a) определение и регистрацию существенных изменений;

b) планирование и тестирование изменений;

c) оценку возможных последствий, включая последствия для безопасности, таких изменений;

d) формализованную процедуру утверждения предполагаемых изменений;

e) подробное информирование об изменениях всех заинтересованных лиц;

f) процедуры возврата в исходный режим, включая процедуры и обязанности в отношении отмены и последующего восстановления в случае неудачных изменений и непредвиденных обстоятельств.

С целью обеспечения уверенности в надлежащем контроле всех изменений в оборудовании, программном обеспечении или процедурах, должна быть формально определена ответственность и разработаны соответствующие процедуры управления. При внесении изменений вся необходимая информация должна сохраняться в контрольном журнале.

Дополнительная информация

Неадекватный контроль изменений средств и систем обработки информации — распространенная причина системных сбоев и инцидентов безопасности. Изменения эксплуатационной среды, особенно при переходе от стадии разработки к стадии эксплуатации, могут оказывать влияние на надежность прикладных программ (см. 12.5.1).

Изменения эксплуатируемых систем следует осуществлять только в том случае, если на это имеется обоснованная причина, затрагивающая бизнес, например возрастание риска в отношении системы. Обновление систем новейшими версиями эксплуатируемой системы или прикладных программ не всегда отвечает интересам бизнеса, поскольку оно может привнести большее число уязвимостей и бóльшую нестабильность, чем действующая версия. Могут также потребоваться дополнительное обучение, расходы на лицензирование, поддержка, сопровождение и административный надзор, а также аппаратные средства, особенно в течение периода миграции.

10.1.3 Разделение обязанностей

Мера и средство контроля и управления

Обязанности и области ответственности должны быть разделены для уменьшения возможностей неавторизованной или непреднамеренной модификации активов организации или их нецелевого использования.

Рекомендация по реализации

Разделение обязанностей — это способ сведения к минимуму риска нецелевого использования систем вследствие ошибочных или злонамеренных действий пользователей. Необходимо предпринять определенные меры предосторожности, чтобы ни один сотрудник не мог осуществлять доступ, модифицировать или использовать активы, не имея авторизации или не будучи обнаруженным. Инициирование события должно быть отделено от его авторизации. При разработке мер и средств контроля и управления следует учитывать опасность сговора.

Небольшие организации могут признавать разделение обязанностей труднодостижимым, однако, данный принцип должен быть применен насколько это возможно. В случаях, когда разделение обязанностей осуществить затруднительно, следует рассматривать использование альтернативных мер и средств контроля и управления, таких как мониторинг деятельности, использование контрольных записей, а также надзор со стороны руководства. В то же время важно, чтобы аудит безопасности оставался независимым.

10.1.4 Разделение средств разработки, тестирования и эксплуатации

Мера и средство контроля и управления

Чтобы снизить риски неавторизованного доступа или изменений эксплуатируемой системы, следует обеспечивать разделение средств разработки, тестирования и эксплуатации.

Рекомендация по реализации

Уровень разделения между средами эксплуатации, тестирования и разработки, необходимый для предотвращения проблем эксплуатации, должен быть определен и при этом должны быть реализованы соответствующие меры и средства контроля и управления.

Необходимо рассмотреть следующие вопросы:

a) правила перевода программного обеспечения из статуса разрабатываемого в статус принятого к эксплуатации должны быть определены и документально оформлены;

b) разработка и эксплуатация программного обеспечения должна осуществляться на различных системах или компьютерах в различных доменах или директориях;

c) компиляторы, редакторы и другие инструментальные средства разработки или системные утилиты не должны быть доступны в среде эксплуатации без крайней необходимости;

d) среда системы тестирования должна эмулировать среду эксплуатации настолько точно, насколько это возможно;

e) чтобы уменьшить риск ошибок, пользователи должны применять различные параметры пользователя для эксплуатируемых и тестовых систем, а в экранных меню должны показываться соответствующие идентификационные сообщения;

f) чувствительные данные не должны копироваться в среду системы тестирования (см. 12.4.2).

Дополнительная информация

Деятельность, связанная с разработкой и тестированием, может быть причиной серьезных проблем, например нежелательных изменений файлов или системной среды, а также системных сбоев. В этом случае необходимо поддерживать известную и стабильную среду для выполнения комплексного тестирования и предотвращать несанкционированный доступ разработчиков.

Там, где сотрудники, отвечающие за разработку и тестирование, имеют доступ к действующей системе и ее данным, они могут установить неавторизованную и непротестированную программу или изменить рабочие данные. Применительно к ряду систем такая возможность могла бы быть использована для мошенничества или установки непротестированной или вредоносной программы, что может являться причиной серьезных проблем, связанных с эксплуатацией.

Разработчики и специалисты, проводящие тестирование, могут также быть причиной угроз конфиденциальности эксплуатационной информации. Кроме того, если разработка и тестирование производятся в одной компьютерной среде, это может стать причиной непреднамеренных изменений программного обеспечения или информации. Следовательно, разделение средств разработки, тестирования и эксплуатации целесообразно для уменьшения риска случайного изменения или неавторизованного доступа к программному обеспечению и данным бизнеса среды эксплуатации (см. 12.4.2 на предмет защиты тестовых данных).

10.2 Менеджмент оказания услуг третьей стороной

Цель: Реализовывать и поддерживать соответствующий уровень информационной безопасности и оказания услуг в соответствии с договорами об оказании услуг третьей стороной.

Организация должна проводить проверку реализации договоров, осуществлять мониторинг соответствия условиям договоров и управление изменениями для обеспечения уверенности в том, что оказанные услуги удовлетворяют всем требованиям, согласованным с третьей стороной.

10.2.1 Предоставление услуг

Мера и средство контроля и управления

Необходимо обеспечивать уверенность в том, что меры и средства контроля и управления безопасности, определение услуг и уровни предоставления услуг, включенные в договор о предоставлении услуг третьей стороной, реализуются, функционируют и поддерживаются третьей стороной.

Рекомендация по реализации

Предоставление услуг третьей стороной должно включать согласованные меры по обеспечению безопасности, определению услуг и аспекты менеджмента услуг. Что касается договоров аутсорсинга, организация должна планировать необходимые перемещения (информации, средств обработки информации и др., что должно быть перемещено) и обеспечивать уверенность в том, что безопасность поддерживается на протяжении всего периода перемещения.

Организация должна обеспечивать уверенность в том, что третья сторона поддерживает достаточный объем услуг наряду с реализуемыми планами по обеспечению согласованного уровня непрерывности обслуживания, сохраняемого в случае серьезных отказов обслуживания или бедствия (см. 14.1).

10.2.2 Мониторинг и анализ услуг третьей стороны

Мера и средство контроля и управления

Необходимо регулярно проводить мониторинг и анализ услуг, отчетов и записей, обеспечиваемых третьей стороной, и регулярно проводить аудиты.

Рекомендация по реализации

Мониторинг и анализ услуг, обеспечиваемых третьей стороной, должны обеспечивать уверенность в том, что условия, касающиеся информационной безопасности, и условия договоров соблюдаются, и что менеджмент инцидентов и проблем информационной безопасности осуществляется должным образом. Между организацией и третьей стороной должна существовать связь для того, чтобы:

a) осуществлять мониторинг уровней предоставления услуг с целью проверки соблюдения условий договоров;

b) анализировать отчеты, о предоставлении услуг, подготовленные третьей стороной, и проводить регулярные рабочие встречи в соответствии с договорами;

c) обеспечивать информацию об инцидентах информационной безопасности и анализ данной информации третьей стороной и организацией в соответствии с условиями договоров и любыми поддерживающими руководствами и процедурами;

d) анализировать контрольные записи третьей стороны и записи событий, связанных с безопасностью, эксплуатационных проблем, отказов, прослеживания недостатков и разрушений, относящихся к предоставляемым услугам;

e) решать все выявленные проблемы и осуществлять их менеджмент.

Ответственность за управление отношениями с третьей стороной следует возлагать на специально назначенного сотрудника или на группу управления услугами. Кроме того, организация должна обеспечивать уверенность в том, что третья сторона берет на себя ответственность за проверку соответствия и исполнения требований договоров. Для мониторинга выполнения требований договора (см. 6.2.3), в частности, требований информационной безопасности, необходимы достаточный технический опыт и ресурсы. Когда в оказании услуг замечены недостатки, следует принимать соответствующие меры.

Организация должна поддерживать достаточный общий контроль и прослеживаемость всех аспектов безопасности чувствительной или критической информации, или средств обработки информации, которые доступны, обрабатываются или управляются третьей стороной. Организация должна обеспечивать уверенность в том, что она поддерживает прослеживаемость деятельности, связанной с безопасностью, например управление изменениями, выявление уязвимостей и сообщение/реагирование на инциденты информационной безопасности с помощью четко определенного процесса, формата и структуры отчетности.

Дополнительная информация

Организация должна быть осведомлена о том, что основная ответственность за информацию, обрабатываемую третьей стороной в рамках договоров аутсорсинга, остается за организацией.

10.2.3 Управление изменениями услуг третьей стороны

Мера и средство контроля и управления

Изменения в предоставлении услуг, включая поддержку и улучшение существующих политик, процедур, мер и средств контроля и управления информационной безопасности, должны осуществляться с учетом критичности затрагиваемых систем и процессов бизнеса, а также переоценки рисков.

Рекомендация по реализации

Процесс управления изменениями услуг третьей стороны, должен учитывать:

a) изменения, проводимые организацией, для реализации:

1) улучшения предлагаемых текущих услуг;

2) разработки каких-либо новых прикладных программ и систем;

3) модификаций или обновлений политик и процедур организации;

4) новых мер и средств контроля и управления для устранения инцидентов информационной безопасности и повышения безопасности;

b) изменения в услугах третьей стороны, для реализации:

1) изменений и улучшений в отношении сетей;

2) использования новых технологий;

3) использования новых продуктов или новейших версий/выпусков;

4) новых инструментальных средств и сред разработки;

5) изменений физического расположения средств обслуживания;

6) смены поставщиков.

10.3 Планирование и приемка систем

Цель: Свести к минимуму риск сбоев в работе систем.

Предварительное планирование и подготовка необходимы для обеспечения адекватной производительности и ресурсов, чтобы получить требуемые эксплуатационные данные системы.

Необходимо составить прогноз в отношении требований и перспективной производительности систем с целью снижения риска их перегрузки.

Эксплуатационные требования для новых систем должны быть определены, документально оформлены и протестированы перед их приемкой и использованием.

10.3.1 Управление производительностью

Мера и средство контроля и управления

Использование ресурсов необходимо прогнозировать, исходя из будущих требований к производительности, настраивать и контролировать, чтобы обеспечить уверенность в достижении требуемых эксплуатационных данных системы.

Рекомендация по реализации

Для каждой новой и продолжающейся деятельности необходимо определять требования к производительности. Следует проводить настройку и контроль систем для обеспечения, где необходимо,

уверенности в повышении доступности и эффективности систем. Необходимо применять выявляющие меры и средства контроля и управления, своевременно указывающие на проблемы. Прогнозирование требований к производительности должно учитывать новые требования бизнеса и новые системные требования, а также текущие и прогнозируемые тенденции в отношении возможностей обработки информации организации.

Особое внимание необходимо уделять любым ресурсам, требующим длительного времени на закупку или больших расходов, поэтому руководителям следует осуществлять контроль использования ключевых системных ресурсов. Они должны определять тенденции в использовании, в частности, касающиеся прикладных программ для бизнеса или инструментальных средств информационных систем управления.

Руководителям следует использовать эту информацию с целью выявления потенциально узких мест и зависимости от ключевого персонала, который мог бы представлять угрозу безопасности систем или сервисов, и планирования соответствующего действия.

10.3.2 Приемка систем

Мера и средство контроля и управления

Должны быть определены критерии приемки для новых информационных систем, обновлений и новых версий, кроме того, необходимо тестировать системы в течение их разработки и перед их приемкой.

Рекомендация по реализации

Руководители должны обеспечить уверенность в том, что требования и критерии для принятия новых систем четко определены, согласованы, документально оформлены и протестированы. Новые информационные системы, обновления и новые версии должны вводиться в эксплуатацию только после прохождения официальной приемки. До официальной приемки необходимо рассмотреть следующие аспекты:

a) требования к мощности и производительности компьютера;

b) процедуры восстановления после сбоев и перезапуска, и планы действий в чрезвычайных ситуациях;

c) подготовка и тестирование типовых операционных процедур на соответствие установленным стандартам;

d) наличие согласованного набора меры и средства контроля и управления безопасности;

e) эффективные ручные процедуры;

f) мероприятия по обеспечению непрерывности бизнеса (см. 14.1);

g) документальное подтверждение того, что внедрение новой системы не будет неблагоприятно влиять на существующие системы, особенно, во время максимальных нагрузок, например в конце месяца;

h) документальное подтверждение того, что было учтено влияние, оказываемое новой системой, на общую безопасность организации;

i) тренинг в отношении эксплуатации и использования новых систем;

j) простота использования, поскольку это влияет на производительность работы пользователя и позволяет избегать ошибок оператора.

В отношении новых крупных разработок, службы поддержки и пользователи должны привлекаться для консультации на всех стадиях процесса разработки с целью эффективного проектирования системы. Соответствующие тесты должны проводиться для подтверждения того, что все критерии приемки удовлетворены полностью.

Дополнительная информация

Приемка может включать формальный процесс сертификации и аккредитации для подтверждения того, что требования к безопасности были учтены должным образом.

10.4 Защита от вредоносной и мобильной программы

Цель: Защита целостности программного обеспечения и информации.

Необходимо принимать меры предосторожности для предотвращения и обнаружения вредоносной программы и неавторизованной мобильной программы.

Программное обеспечение и средства обработки информации уязвимы по отношению к внедрению вредоносной программы, такой как компьютерные вирусы, сетевые «черви», «троянские кони» и логические бомбы. Пользователи должны быть осведомлены об опасности, связанной с вредоносной программой. Руководители должны, при необходимости, обеспечить внедрение мер и средств контроля и управления с целью предотвращения, обнаружения и удаления вредоносной программы и контролирования мобильной программы.

10.4.1 Меры и средства контроля и управления против вредоносной программы

Мера и средство контроля и управления

Необходимо внедрить меры и средства контроля и управления, связанные с обнаружением, предотвращением и восстановлением, с целью защиты от вредоносной программы, а также процедуры, обеспечивающие соответствующую осведомленность пользователей.

Рекомендация по реализации

Защита от вредоносной программы должна основываться: на обнаружении вредоносной программы и восстановлении программного обеспечения; на понимании требований безопасности; на мерах и средствах контроля и управления соответствующего доступа к системе и менеджмента изменений. Необходимо рассмотреть следующие рекомендации:

a) создать официальную политику, устанавливающую запрет на использование неавторизованного программного обеспечения (см. 15.1.2);

b) создать официальную политику защиты от рисков, связанных с получением файлов и программного обеспечения, либо из внешних сетей, либо через другие передающие среды, показывающую, какие защитные меры следует принять;

c) проводить регулярный анализ программного обеспечения и содержания данных систем, поддерживающих критические процессы бизнеса; необходима формальная процедура расследования причин наличия любых неавторизованных или измененных файлов;

d) осуществлять в качестве превентивной меры или обычным порядком инсталляцию и регулярное обновление программного обеспечения по обнаружению вредоносной программы и восстановлению для сканирования компьютеров и носителей информации; проводимые проверки должны включать:

1) проверку на наличие вредоносной программы любых файлов на электронных или оптических носителях и файлов, полученных из сетей перед их использованием;

2) проверку любых вложений электронной почты и скачиваемой информации до их использования на наличие вредоносной программы; эта проверка должна выполняться в разных точках, например на серверах электронной почты, настольных компьютерах или при входе в сеть организации;

3) проверку web-страниц на наличие вредоносной программы;

e) определять управленческие процедуры и обязанности, связанные с защитой от вредоносной программы в системах, тренинг их использования, оповещение и восстановление после атак вредоносной программы (см. 13.1 и 13.2);

f) подготовить соответствующие планы по обеспечению непрерывности бизнеса в части восстановления после атак вредоносной программы, включая все необходимые мероприятия по резервированию и восстановлению данных и программного обеспечения (см. раздел 14);

g) реализовать процедуры регулярного сбора информации, например подписываясь на список почтовой рассылки и (или) проверяя web-сайты, дающие информацию о новой вредоносной программе;

h) реализовать процедуры проверки информации, касающейся вредоносной программы, и обеспечить точность и информативность предупредительных сообщений; соответствующие руководители должны обеспечить уверенность в том, что компетентные источники, например информация из известных журналов, заслуживающих доверия Интернет-сайтов или от поставщиков антивирусного программного обеспечения используется для определения различий между ложной и реальной вредоносной программой; все пользователи должны быть осведомлены о проблеме ложных вирусов и действиях при их получении.

Дополнительная информация

Использование двух или более программных продуктов, обеспечивающих защиту от вредоносной программы в среде обработки информации, от разных поставщиков может повысить эффективность данной защиты.

Для защиты от вредоносной программы может устанавливаться программное обеспечение, позволяющее проводить автоматические обновления определенных файлов и сканирование машин для подтверждения актуальности защиты. Кроме того, такое программное обеспечение может быть установлено на каждом рабочем столе для выполнения автоматических проверок.

Следует заботиться о защите от внедрения вредоносной программы во время процедур по техническому обслуживанию и процедур, связанных с критическими ситуациями, когда можно обойти обычные меры и средства контроля и управления, применяемые для защиты от вредоносной программы.

10.4.2 Меры и средства контроля и управления при использовании мобильной программы

Мера и средство контроля и управления

Там, где разрешено использование мобильной программы, конфигурация должна обеспечивать уверенность в том, что разрешенная мобильная программа функционирует в соответствии с ясно сформулированной политикой безопасности, а исполнение неразрешенной мобильной программы будет запрещено.

Рекомендация по реализации

Для предотвращения выполнения мобильной программой неразрешенных действий необходимо принимать следующие меры:

a) обеспечивать выполнение мобильной программы в логически изолированной среде;

b) блокировать любое несанкционированное использование мобильной программы;

c) блокировать прием мобильной программы;

d) активизировать технические меры, доступные в отношении определенной системы, чтобы обеспечить уверенность в управляемости мобильной программы;

e) контролировать ресурсы, доступные мобильной программе;

f) применять криптографические меры и средства контроля и управления для однозначной аутентификации мобильной программы.

Дополнительная информация

Мобильная программа представляет собой программный код, который переходит с одного компьютера на другой, а затем исполняется автоматически, и выполняет определенную функцию без какого-либо взаимодействия с пользователем или при минимальном взаимодействии с ним. Мобильная программа связана с рядом услуг вспомогательного программного обеспечения.

В дополнение к обеспечению уверенности в том, что мобильная программа не содержит вредоносного кода, важно контролировать мобильную программу с целью предотвращения неавторизованного использования или разрушения системных, сетевых или прикладных ресурсов и других нарушений информационной безопасности.

10.5 Резервирование

Цель: Поддерживать целостность и доступность информации и средств обработки информации.

Должны быть созданы типовые процедуры по реализации установленной политики и стратегии резервирования (см. 14.1) в отношении снятия резервных копий данных и обеспечения их своевременного восстановления.

10.5.1 Резервирование информации

Мера и средство контроля и управления

Резервное копирование информации и программного обеспечения должно выполняться и тестироваться на регулярной основе в соответствии с установленной политикой резервирования.

Рекомендация по реализации

Следует обеспечить адекватные средства резервирования для обеспечения уверенности в том, что вся важная информация и программное обеспечение могут быть восстановлены после бедствия или сбоя оборудования.

В отношении резервирования информации необходимо рассматривать следующие вопросы:

a) необходимо определить надлежащий уровень резервной информации;

b) необходимо обеспечивать точные и полные записи резервных копий и документально оформленные процедуры восстановления;

c) объем (т. е. полное или выборочное резервирование) и частота резервирования должны отражать требования бизнеса организации, требования к безопасности затрагиваемой информации и критичность информации для непрерывной работы организации;

d) резервные копии должны храниться в удаленном месте, на надежном расстоянии, достаточном, чтобы избежать любого повреждения вследствие аварийной ситуации в основном здании;

e) в отношении резервной информации должен быть обеспечен соответствующий уровень физической защиты и защиты от воздействий окружающей среды (см. 9), в соответствии со стандартами, применяемыми в основном здании; меры и средства контроля и управления, применяемые к носителям информации в основном здании, должны также применяться и на резервной площадке;

f) носители резервной информации должны регулярно тестироваться для обеспечения уверенности в том, что в случае чрезвычайных ситуаций они могут быть использованы;

g) процедуры восстановления следует регулярно проверять и тестировать для обеспечения уверенности в их эффективности, а также в том, что для выполнения этих процедур потребуется не больше времени, чем это определено;

h) в ситуациях, когда конфиденциальность играет важную роль, резервные копии необходимо защищать посредством шифрования.

Мероприятия по резервированию, применяемые в отношении отдельных систем, должны регулярно тестироваться для обеспечения уверенности в том, что они удовлетворяют требованиям, содержащимся в планах непрерывности бизнеса (см. 14). Применительно к критическим системам, мероприятия по резервированию должны охватывать информацию, прикладные программы и данные всех систем, необходимые для восстановления целой системы в случае бедствия.

Следует определить сроки хранения важной информации бизнеса, а также любое требование к архивным копиям, подлежащим длительному хранению (см. 15.1.3).

Дополнительная информация

Для упрощения процесса резервирования и восстановления мероприятия по резервированию могут быть автоматизированы. Такие решения по автоматизации должны в достаточной мере и регулярно тестироваться, прежде чем они будут реализованы.

10.6 Менеджмент безопасности сети

Цель: Обеспечить уверенность в защите информации в сетях и защите поддерживающей инфраструктуры.

Менеджмент безопасности сетей, которые могут проходить за пределами организации, требует пристального внимания к потокам данных, правовым последствиям, мониторингу и защите.

Дополнительные меры и средства контроля и управления могут также потребоваться для защиты чувствительной информации, передаваемой по общедоступным сетям.

10.6.1 Меры и средства контроля и управления сетями

Мера и средство контроля и управления

Сети должны адекватно управляться и контролироваться, чтобы быть защищенными от угроз и обеспечить безопасность систем и прикладных программ, использующих сеть, включая информацию во время ее передачи.

Рекомендация по реализации

Руководители, отвечающие за поддержку сетевых ресурсов, должны внедрять меры и средства контроля и управления для обеспечения уверенности в безопасности информации в сетях и защиты подключенных сервисов от неавторизованного доступа. В частности, необходимо рассмотреть следующие вопросы:

a) следует разделить, где это необходимо, ответственность за поддержку сетевых ресурсов и за поддержку компьютерных операций (см. 10.1.3);

b) следует определить обязанности и процедуры для управления удаленным оборудованием, включая оборудование, установленное у конечных пользователей;

c) специальные меры и средства контроля и управления следует внедрить для обеспечения конфиденциальности и целостности данных, передаваемых по общедоступным сетям, или по беспроводным сетям, а также для защиты подключенных систем и прикладных программ (см. 11.4 и 12.3); специальные меры и средства контроля и управления могут потребоваться для поддержки доступности сетевых сервисов и рабочих станций;

d) соответствующая регистрация и мониторинг должны применяться с целью обеспечения возможности регистрации действий, имеющих значение для безопасности;

e) действия руководства должны быть тщательно согласованы как для оптимизации получаемых организацией услуг, так и для обеспечения уверенности в том, что меры и средства контроля и управления единообразно применимы ко всей инфраструктуре обработки информации.

Дополнительная информация

Дополнительную информацию о сетевой безопасности можно найти в ИСО/МЭК 18028-4 [19].

10.6.2 Безопасность сетевых услуг

Мера и средство контроля и управления

Средства обеспечения безопасности, уровни услуг и требования в отношении менеджмента всех сетевых услуг должны быть определены и включены в любой договор по сетевым услугам, вне зависимости от того, будут ли они обеспечиваться силами организации или в рамках договоров аутсорсинга.

Рекомендация по реализации

Способность провайдера сетевых услуг безопасно осуществлять менеджмент установленных услуг следует определять и подвергать регулярному мониторингу, а право проведения аудита должно быть согласовано.

Должны быть определены меры безопасности, необходимые для конкретных услуг, например средства обеспечения безопасности, уровни услуг и требования в отношении менеджмента. Организация должна обеспечивать уверенность в том, что провайдеры сетевых услуг реализуют эти меры.

Дополнительная информация

Сетевые услуги включают в себя обеспечение соединений, услуг частных сетей и сетей с дополнительными функциями, а также решений, касающихся управления безопасностью сети, например межсетевые экраны и системы обнаружения вторжения. Такие услуги могут варьироваться от простых решений, касающихся неуправляемой пропускной способности, до сложных решений с обеспечением дополнительных услуг.

Средствами обеспечения безопасности сетевых услуг могут быть:

a) средства, применяемые для обеспечения безопасности сетевых услуг, например аутентификация, шифрование, и меры и средства контроля и управления сетевыми соединениями;

b) соблюдение технических параметров, требуемых для безопасного подключения сетевых услуг в соответствии с правилами безопасности сетевых соединений;

c) процедуры использования сетевой услуги, применяемые для ограничения доступа к сетевым услугам или прикладным программам, где это необходимо.

10.7 Обращение с носителями информации

Цель: Предотвратить неавторизованное раскрытие, модификацию, выбытие или уничтожение активов и прерывание деятельности бизнеса.

Использование носителей информации должно контролироваться, необходимо также обеспечить их физическую безопасность.

Должны быть определены соответствующие процедуры в отношении защиты документов, компьютерных носителей информации (например лент, дисков), данных ввода/вывода и системной документации от неавторизованного раскрытия, модификации, выноса и уничтожения.

10.7.1 Менеджмент сменных носителей информации

Мера и средство контроля и управления

Должны существовать процедуры в отношении менеджмента сменных носителей информации.

Рекомендация по реализации

Необходимо рассмотреть следующие рекомендации в отношении менеджмента сменных носителей информации:

a) если не предполагается повторно использовать содержание носителей информации, которые должны быть перемещены за пределы организации, то информацию необходимо сделать неизвлекаемой;

b) где необходимо и практично, должно требоваться разрешение на вынос носителей информации из организации и запись о таком перемещении следует хранить как контрольную запись для аудита;

c) все носители информации должны храниться в надежной, безопасной среде, в соответствии со спецификациями изготовителей;

d) информацию, хранимую на носителях, востребованную дольше, чем жизненный цикл носителя (в соответствии со спецификациями изготовителей), следует хранить также и в другом месте, во избежание потери информации вследствие износа носителей;

e) для уменьшения возможности потери данных должна быть предусмотрена регистрация сменных носителей информации;

f) сменные дисковые накопители разрешается использовать только в случае, обусловленном потребностями бизнеса.

Все процедуры и уровни авторизации должны быть четко зафиксированы документально.

Дополнительная информация

К сменным носителям информации относятся ленты, диски, диски флэш-памяти, сменные жесткие диски, CD, DVD и печатные носители информации.

10.7.2 Утилизация носителей информации

Мера и средство контроля и управления

Носители информации, когда в них больше нет необходимости, следует надежно и безопасно утилизировать, используя формальные процедуры.

Рекомендация по реализации

Формальные процедуры для безопасной утилизации носителей информации должны снижать риск утечки чувствительной информации неавторизованным лицам. Процедуры для безопасной утилизации

носителей, содержащих чувствительную информацию, должны соответствовать чувствительности той информации. Необходимо рассмотреть следующие вопросы:

a) носители, содержащие чувствительную информацию, должны храниться и утилизироваться надежно и безопасно, например посредством сжигания или измельчения; если носители планируется использовать в пределах организации для других прикладных программ, информация на них должна быть уничтожена;

b) должны существовать процедуры по выявлению носителей информации, для которых может потребоваться безопасная утилизация;

c) может оказаться проще принимать меры по сбору и безопасной утилизации в отношении всех носителей информации, чем пытаться выделить носители с чувствительной информацией;

d) многие организации предлагают услуги по сбору и утилизации бумаги, оборудования и носителей информации; следует тщательно выбирать подходящего подрядчика с учетом имеющегося у него опыта и применяемых мер и средств контроля и управления;

e) где возможно, утилизацию носителей, содержащих чувствительную информацию, следует фиксировать как контрольную запись для аудита.

При накоплении носителей информации, подлежащих утилизации, следует принимать во внимание «эффект накопления», т. е. большое количество нечувствительной информации делает ее чувствительной.

Дополнительная информация

Чувствительная информация может быть раскрыта при небрежной утилизации носителей (см. также 9.2.6 на предмет информации об утилизации оборудования).

10.7.3 Процедуры обработки информации

Мера и средство контроля и управления

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

Рекомендация по реализации

Должны быть разработаны процедуры по ручной обработке информации, обработке информации с использованием компьютеров, хранению и передаче информации в соответствии с ее классификацией (см. 7.2). Необходимо рассмотреть следующие вопросы:

a) обработку и маркировку всех носителей информации в соответствии с ее указанным уровнем классификации;

b) ограничение доступа с целью предотвращения доступа неавторизованного персонала;

c) обеспечение формальной регистрации авторизованных получателей данных;

d) обеспечение уверенности в том, что процесс ввода данных и обработки завершаются должным образом и что выполняется проверка выходных данных;

e) защиту информации, находящейся в буфере данных и ожидающей вывода, соответствующую степени чувствительности этой информации;

f) хранение носителей информации в соответствии со спецификациями изготовителей;

g) сведение распространения данных к минимуму;

h) четкая маркировка всех копий данных, предназначенных вниманию авторизованного получателя;

i) пересмотр списков рассылки и списков авторизованных получателей через регулярные интервалы времени.

Дополнительная информация

Эти процедуры применяются к информации в документах, вычислительным системам, сетям, переносным компьютерам, мобильным средствам связи, почте, речевой почте, речевой связи вообще, мультимедийным устройствам, почтовым услугам/устройствам, к использованию факсов и любых других чувствительных объектов, например бланков чеков и счетов.

10.7.4 Безопасность системной документации

Мера и средство контроля и управления

Системная документация должна быть защищена от неавторизованного доступа.

Рекомендация по реализации

Для защиты системной документации необходимо учитывать следующие вопросы:

a) системную документацию надлежит хранить безопасным образом;

b) список лиц, имеющих доступ к системной документации, необходимо свести к минимуму; доступ должен быть авторизован владельцем прикладной программы;

c) системную документацию, полученную или поддерживаемую через общедоступную сеть, следует защищать надлежащим образом.

Дополнительная информация

Системная документация может содержать разнообразную чувствительную информацию, например описание процессов работы прикладных программ, процедур, структур данных, процессов авторизации.

10.8 Обмен информацией

Цель: Поддерживать безопасность информации и программного обеспечения, обмениваемых в пределах организации и с любым внешним объектом.

Обмен информацией и программным обеспечением между организациями должен основываться на формальной политике обмена, осуществляться в соответствии с соглашениями по обмену и соответствовать действующему законодательству (см. 15).

Необходимо определить процедуры и стандарты по защите информации и ее физических носителей при передаче.

10.8.1 Политики и процедуры обмена информацией

Мера и средство контроля и управления

Должны существовать формальные политики, процедуры и меры и средства контроля и управления в отношении обмена информацией с целью защиты такого обмена, когда используются все типы средств связи.

Рекомендация по реализации

Процедуры, меры и средства контроля и управления, которые необходимо соблюдать при использовании электронных средств связи для обмена информацией, должны учитывать следующее:

a) процедуры, предназначенные для защиты обмениваемой информации от перехвата, копирования, модификации, ложной маршрутизации и разрушения;

b) процедуры обнаружения вредоносной программы, которая может передаваться при использовании электронных средств связи, и процедуры защиты от неё (см. 10.4.1);

c) процедуры защиты передаваемой чувствительной электронной информации, имеющей форму приложения;

d) политику или рекомендации, определяющие приемлемое использование электронных средств связи (см. 7.1.3);

e) процедуры использования беспроводной связи, учитывая сопряженные с ней определенные риски;

f) обязательство сотрудника, подрядчика и любого другого представителя не компрометировать организацию, например посредством клеветы, антисоциальных действий, выдачи себя за другое лицо, распространения «писем счастья», использования «тайных рычагов» и т. д.;

g) использование криптографических методов, например для защиты конфиденциальности, целостности и аутентичности информации (см. 12.3);

h) рекомендации по сохранению и утилизации всей деловой корреспонденции, включая сообщения, в соответствии с действующими национальными и местными законодательными и нормативными актами;

i) напоминание сотрудникам о том, что нельзя оставлять чувствительную или критическую информацию на печатающих устройствах, например копировальных устройствах, принтерах и факсах, поскольку неавторизованный персонал может осуществлять к ним доступ;

j) меры и средства контроля и управления и ограничения, связанные с пересылкой средств связи, например автоматическая пересылка электронной почты на внешние почтовые адреса;

k) напоминание сотрудникам о необходимости соблюдения мер предосторожности, например не следует разглашать чувствительную информацию во избежание ее подслушивания или перехвата при телефонных звонках:

1) лицами, находящимися в непосредственной близости, особенно при использовании мобильных телефонов;

2) при прослушивании телефонных переговоров и других формах подслушивания путем физического доступа к трубке или телефонной линии, или при использовании сканирующих приемников;

3) посторонними лицами на стороне адресата;

l) напоминание сотрудникам о том, что нельзя оставлять сообщения, содержащие чувствительную информацию, на автоответчиках, поскольку они могут быть прослушаны неавторизованными лицами, храниться в общественных системах или неверно помещены на хранение вследствие ошибки соединения;

m) напоминание сотрудникам о проблемах, связанных с использованием факсов, 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 ошибки в наборе, либо из-за использования неправильно сохраненного номера;

n) напоминание сотрудникам о том, что не следует регистрировать демографические данные, например адрес электронной почты или другую личную информацию, в каком-либо программном обеспечении, во избежание ее сбора для неавторизованного использования;

o) напоминание сотрудникам о том, что современные факсимильные и фотокопирующие устройства оснащены страничной кэш-памятью, и «запоминают» страницы в случае проблем с бумагой или передачей, которые будут напечатаны после устранения неисправности.

Кроме того, необходимо напоминать сотрудникам о том, что не следует вести конфиденциальные беседы в общественных местах или открытых офисах, а также в переговорных комнатах, стены которых не защищены звукоизоляцией.

Средства обмена информацией должны соответствовать любым действующим законодательным требованиям (см. 15).

Дополнительная информация

Обмен информацией может осуществляться при использовании различных типов коммуникационных средств, включая электронную почту, факсимильные, аудио- и видео- средства.

Обмен программным обеспечением может осуществляться при использовании различных типов носителей информации, включая «скачивание» из Интернета и приобретение у поставщиков, продающих готовые продукты.

Следует учитывать подразумеваемые положения бизнеса, законодательства и безопасности, связанные с электронным обменом данными, электронной торговлей и электронными коммуникациями, а также и с требованиями к мерам и средствам контроля и управления.

Информация может быть скомпрометирована из-за недостатка осведомленности сотрудников в отношении политики или процедур по использованию средств обмена информацией, например вследствие подслушивания при переговорах по мобильному телефону в общественном месте, отправления сообщения электронной почты по неправильному адресу, прослушивания автоответчиков, неавторизованного доступа к системам голосовой почты или случайной отсылки факсимильных сообщений неправильному адресату.

Операции бизнеса могут быть прерваны и информация может быть скомпрометирована в случае отказа, перегрузки или прерывания в работе средств связи (см. 10.3 и 14). Информация может быть скомпрометирована вследствие доступа неавторизованных пользователей (см. 11).

10.8.2 Соглашения по обмену информацией

Мера и средство контроля и управления

Необходимо заключать соглашения по обмену информацией и программным обеспечением между организацией и сторонними организациями.

Рекомендация по реализации

В соглашениях по обмену следует учитывать следующие условия безопасности:

a) обязанности руководства в отношении контроля и уведомления о передаче, отправке и получении;

b) процедуры уведомления отправителя, а также процедуры передачи, отправки и получения;

c) процедуры обеспечения прослеживаемости и неотказуемости;

d) минимальные требования технических стандартов по формированию и передаче пакетов данных;

e) соглашения в отношении передачи на хранение исходных пакетов данных;

f) стандарты в отношении курьерской службы;

g) ответственность и обязательства в случае инцидентов информационной безопасности, например в случае потери данных;

h) использование согласованной системы маркировки для критической или чувствительной информации, обеспечивающей уверенность в том, что значение этой маркировки будет сразу же понято и что информация будет соответственно защищена;

i) право собственности и обязанности по защите данных, соблюдение авторских прав, соответствие лицензии на программное обеспечение и аналогичные требования (см. 15.1.2 и 15.1.4);

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

k) любые специальные меры и средства контроля и управления, которые могут потребоваться для защиты чувствительных элементов, например криптографических ключей (см. 12.3).

Необходимо создавать и поддерживать политики, процедуры и стандарты в отношении защиты информации и физических носителей информации при их пересылке (см. также 10.8.3), а в соглашении по обмену следует делать на них ссылку.

Содержание любого соглашения в части безопасности должно отражать чувствительность затрагиваемой информации бизнеса.

Дополнительная информация

Соглашения могут существовать в электронном или физическом виде и могут иметь форму официальных договоров или условий найма. В отношении чувствительной информации, определенные механизмы, используемые для обмена такой информацией, должны быть единообразны для всех организаций и типов соглашений.

10.8.3 Физические носители информации при транспортировке

Мера и средство контроля и управления

Носители информации должны быть защищены от неавторизованного доступа, неправильного использования или повреждения во время их транспортировки за пределами организации.

Рекомендация по реализации

Для защиты носителей информации, передаваемых между различными пунктами назначения, необходимо учитывать следующие рекомендации:

a) необходимо пользоваться услугами надежных перевозчиков или курьеров;

b) список авторизованных курьеров необходимо согласовывать с руководством;

c) необходимо разработать процедуры для проверки идентификации курьеров;

d) упаковка должна быть достаточно прочной для защиты от любого физического повреждения, которое, вероятно, может иметь место при транспортировке, и соответствовать любым требованиям изготовителей (например программного обеспечения), необходимо обеспечивать защиту от воздействия любых факторов окружающей среды, которые могут снизить эффективность восстановления, таких как тепловой эффект, влажность или электромагнитные поля;

e) меры и средства контроля и управления следует применять, где это необходимо, для защиты чувствительной 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, разбивка отправления на несколько частей, пересылаемых различными маршрутами.

Дополнительная информация

Информация может быть уязвимой вследствие неавторизованного доступа, неправильного использования или искажения во время физической транспортировки, например при пересылке носителей информации по почте или через курьера.

10.8.4 Электронный обмен сообщениями

Мера и средство контроля и управления

Необходимо должным образом защищать информацию, включаемую в электронный обмен сообщениями.

Рекомендация по реализации

В отношении электронного обмена сообщениями, необходимо учитывать следующие вопросы, связанные с обеспечением безопасности:

a) защита сообщений от неавторизованного доступа, модификации или отказа в обслуживании;

b) обеспечение правильной адресации и передачи сообщения;

c) общая надежность и доступность услуг;

d) законодательные вопросы, например требования в отношении использования электронных подписей;

e) получение одобрения до использования внешних общедоступных услуг, таких как мгновенный обмен сообщениями или разделение файлов;

f) строгие уровни аутентификации управления доступом со стороны общедоступных сетей.

Дополнительная информация

Электронный обмен сообщениями, например электронная почта, обмен данными в электронном виде и мгновенный обмен сообщениями, играет все более важную роль в коммуникациях бизнеса. Риски, связанные с электронным обменом сообщениями, отличаются от рисков, присущих передаче сообщений на бумаге.

10.8.5 Информационные системы бизнеса

Мера и средство контроля и управления

Необходимо разработать и внедрить политики и процедуры защиты информации, связанной с взаимодействием информационных систем бизнеса.

Рекомендация по реализации

Необходимо учитывать последствия от взаимодействия информационных систем для безопасности и бизнеса в целом, такие как:

a) известная уязвимость, присущая административным системам и системам учета и отчетности, где информация разделяется между различными частями организации;

b) уязвимость информации в системах связи бизнеса, например записи телефонных разговоров или переговоров по конференц-связи, конфиденциальность звонков, хранение факсов, вскрытие и рассылка электронных сообщений;

c) политика и соответствующие меры и средства контроля и управления для менеджмента совместного использования информации;

d) запрет на использование чувствительной информации бизнеса и не подлежащих оглашению документов, если данные системы не обеспечивают соответствующий уровень защиты (см. 7.2);

e) ограничение доступа к данным личных ежедневников отдельных сотрудников, например работающих над чувствительными проектами;

f) определение категорий тех сотрудников, подрядчиков или деловых партнеров, которым разрешено использовать систему, и точек, с которых может осуществляться доступ к ней (см. 6.2);

g) ограничение отдельных возможностей системы для определенных категорий пользователей;

h) определение статуса пользователей, например сотрудников организации или подрядчиков, в отдельных директориях, для удобства других пользователей;

i) сохранение и резервное копирование информации, содержащейся в системе (см. 10.5.1);

j) условия перехода на аварийный режим работы и перечень соответствующих мероприятий (см. 14).

Дополнительная информация

Офисные информационные системы обеспечивают возможность быстрого распространения и совместного использования информации бизнеса и представляют собой комбинацию документов, компьютеров, переносных компьютеров, мобильных средств связи, почты, голосовой почты, речевой связи, мультимедийных систем, услуг доставки почтовых отправлений и факсов.

10.9 Услуги электронной торговли

Цель: Обеспечить уверенность в безопасности услуг электронной торговли и их безопасном использовании.

Следует учитывать последствия для безопасности, связанные с использованием услуг электронной торговли, включая транзакции в режиме онлайн, и необходимость мер и средств контроля и управления. Необходимо рассматривать также целостность и доступность информации, публикуемой электронным образом при использовании общедоступных сетей.

10.9.1 Электронная торговля

Мера и средство контроля и управления

Информация, используемая в электронной торговле, проходящая по общедоступным сетям, должна быть защищена от мошенничества, оспаривания договоров, а также неавторизованного раскрытия и модификации.

Рекомендация по реализации

В отношении электронной торговли необходимо рассмотреть следующие вопросы в области безопасности:

a) степень защищенности каждой стороны при идентификации друг друга, например посредством аутентификации;

b) процессы авторизации в отношении того, кто может устанавливать цены, выпускать или подписывать ключевые коммерческие документы;

c) обеспечение уверенности в том, что торговые партнеры полностью проинформированы о своих авторизациях;

d) определение и удовлетворение требований в отношении конфиденциальности, целостности, подтверждения отправки и получения ключевых документов, а также невозможности отказа от совершенных сделок, например связанных с процессами заключения контрактов и проведения тендеров;

e) уровень доверия, вкладываемого в достоверность рекламируемых прайс-листов;

f) конфиденциальность любых чувствительных данных или информации;

g) конфиденциальность и целостность любой информации о сделках, связанных с заказом, условиях оплаты и адресах поставки, а также подтверждения при его получении;

h) степень контроля, достаточная для проверки информации об оплате, представленной клиентом;

i) выбор формы оплаты, наиболее защищенной от мошенничества;

j) уровень защиты, необходимый для обеспечения конфиденциальности и целостности информации о заказах;

k) предотвращение потери или дублирования информации о сделках;

l) ответственность за любые мошеннические сделки;

m) страховые требования.

Многие из вышеупомянутых проблем могут быть решены с использованием криптографических мер и средств контроля и управления (см. 12.3), при этом необходимо обеспечить соответствие требованиям законодательства (см. 15.1, особенно 15.1.6, относительно законодательства в области криптозащиты).

Соглашения в области электронной торговли между партнерами следует подкреплять документально оформленными договорами, которые устанавливают согласованные между сторонами условия заключения сделок, включая подробную процедуру авторизации (см. перечисление b) 10.9.1). Могут потребоваться также дополнительные соглашения с поставщиками сетевых и информационных услуг.

Общественные системы торговли должны обнародовать условия заключения сделок с клиентами.

Необходимо обеспечить устойчивость к компьютерным атакам на основной(ые) сервер(ы) электронной торговли, а также рассмотреть последствия для безопасности всех сетевых взаимосвязей, необходимых для реализации решений электронной торговли (см. 11.4.6).

Дополнительная информация

Электронная торговля уязвима по отношению к сетевым угрозам, которые могут привести к краже, оспариванию договоров, а также к раскрытию или модификации информации.

Для снижения рисков электронная торговля может воспользоваться заслуживающими доверия методами аутентификации, например использующими криптографию с открытым ключом и цифровые подписи (см. 12.3). Там, где необходимо, могут использоваться услуги третьей доверенной стороны.

10.9.2 Транзакции в режиме онлайн

Мера и средство контроля и управления

Информацию, используемую в онлайн транзакциях, следует защищать для предотвращения неполной передачи, неправильной маршрутизации, неавторизованного изменения сообщений, неавторизованного раскрытия, неавторизованного дублирования или воспроизведения сообщений.

Рекомендация по реализации

Вопросы безопасности транзакций в режиме онлайн должны включать:

a) использование электронных подписей каждой из сторон, участвующих в транзакции;

b) все аспекты транзакции, т. е. обеспечение уверенности в том, что:

1) пользовательские мандаты всех сторон действительны и проверены;

2) транзакция остается конфиденциальной;

3) приватность всех участвующих сторон сохраняется;

c) канал связи между всеми участвующими сторонами зашифрован;

d) протоколы, используемые для установления связи между всеми участвующим сторонами, защищены;

e) обеспечение уверенности в том, что хранение деталей транзакции обеспечивается за пределами любой общедоступной среды, например на платформе хранения, имеющейся в Интернете организации, а не в среде хранения, доступной непосредственно из Интернета;

f) там, где используются услуги доверенного органа (например в целях создания и поддержки цифровых подписей и (или) цифровых сертификатов), безопасность обеспечивается как интегрированная и неотъемлемая часть на протяжении всего сквозного процесса менеджмента подписей/сертификатов.

Дополнительная информация

Объем применяемых мер и средств контроля и управления необходимо соизмерять с уровнем риска, связанным с каждой формой онлайн транзакции.

Может возникнуть необходимость соблюдения законов, правил и нормативов в рамках той юрисдикции, в которой транзакция формируется, обрабатывается, завершается и (или) хранится.

Существует много транзакций, которые могут быть выполнены онлайн способом, например контрактные, финансовые и другие.

10.9.3 Общедоступная информация

Мера и средство контроля и управления

Целостность информации, которая доступна в общедоступной системе, следует защищать для предотвращения неавторизованной модификации.

Рекомендация по реализации

Программное обеспечение, данные и другая информация, для которых требуется высокий уровень целостности и которые доступны в общедоступной системе, необходимо защищать с помощью соответствующих механизмов, например цифровых подписей (см. 12.3). Общедоступная система должна быть протестирована на предмет недостатков и отказов прежде, чем информация станет доступной.

Должен применяться формальный процесс утверждения прежде, чем информация станет общедоступной. Кроме того, все материалы, представленные в систему извне, должны быть проверены и утверждены.

Системы электронной публикации, особенно те, которые предоставляют возможности обратной связи и непосредственного ввода информации, должны находиться под тщательным контролем, с тем чтобы:

a) информация была получена в соответствии со всеми требованиями законодательства в отношении защиты данных (см. 15.1.4);

b) информация, введенная в систему электронной публикации, обрабатывалась полностью, точно и своевременно;

c) чувствительная информация должна быть защищена в процессе ее сбора, обработки и хранения;

d) доступ к системе электронной публикации исключал возможность непреднамеренного доступа к сетям, с которыми она связана.

Дополнительная информация

Информацию, размещенную в общедоступной системе, например на доступном через Интернет Web-сервере, возможно, будет необходимо привести в соответствие с законами, правилами и нормами той юрисдикции, в которой находится система, где осуществляется торговля или где проживает(ют) владелец(льцы). Неавторизованная модификация опубликованной электронным способом информации может нанести вред репутации организации, разместившей эту информацию.

10.10 Мониторинг

Цель: Обнаружение неавторизованных действий, связанных с обработкой информации.

Системы должны контролироваться и события информационной безопасности должны быть зарегистрированы. Для обеспечения уверенности в том, что проблемы информационной системы выявляются, следует вести журналы эксплуатации и регистрировать неисправности.

Организация должна выполнять все действующие правовые требования, применимые к ее деятельности, связанной с мониторингом и регистрацией.

Мониторинг систем следует проводить с целью проверки эффективности применяемых мер и средств контроля и управления, а также подтверждения следования модели политики доступа.

10.10.1 Контрольная регистрация

Мера и средство контроля и управления

Необходимо вести и хранить в течение согласованного периода времени контрольные журналы, регистрирующие действия пользователей, нештатные ситуации и события информационной безопасности, чтобы помочь в будущих расследованиях и проведении контроля управления доступом.

Рекомендация по реализации

Контрольные журналы должны включать, при необходимости:

a) идентификаторы пользователей;

b) даты, время и детали ключевых событий, например начало сеанса и завершение сеанса;

c) идентичность и местоположение терминала, если это возможно;

d) регистрацию успешных и отклоненных попыток доступа к системе;

e) регистрацию успешных и отклоненных попыток доступа к данным или другим ресурсам;

f) изменения конфигурации системы;

g) использование привилегий;

h) использование системных утилит и прикладных программ;

i) файлы, к которым был осуществлен доступ и вид доступа;

j) сетевые адреса и протоколы;

k) сигналы тревоги, подаваемые системой управления доступом;

l) активация и деактивация систем защиты, например антивирусных систем и систем обнаружения вторжения.

Дополнительная информация

Контрольные журналы могут содержать данные о вторжениях и конфиденциальные личные данные. Необходимо принимать соответствующие меры для защиты приватности (см. также 15.1.4). Где возможно, системным администраторам следует запрещать стирать или деактивировать журналы регистрации их собственных действий (см. 10.1.3).

10.10.2 Использование системы мониторинга

Мера и средство контроля и управления

Необходимо создать процедуры для проведения мониторинга использования средств обработки информации и регулярно анализировать результаты деятельности, связанной с мониторингом.

Рекомендация по реализации

Уровень мониторинга, необходимый для отдельных средств, следует определять с помощью оценки риска. Организация должна выполнять все действующие законодательные требования, применимые к ее деятельности, связанные с мониторингом. Необходимо рассмотреть следующие аспекты:

a) авторизованный доступ, включая детали, такие как:

1) идентификаторы пользователей;

2) дату 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, привилегированного пользователя, администратора;

2) запуск и остановка системы;

3) подсоединение/отсоединение устройства ввода/вывода;

c) попытки неавторизованного доступа, такие как:

1) неудавшиеся или отклоненные действия пользователей;

2) неудавшиеся или отклоненные действия, затрагивающие данные или 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) предупреждения или сообщения пульта управления;

2) изъятие системного журнала;

3) предупредительные сигналы, связанные с управлением сетью;

4) предупредительные сигналы, подаваемые системой управления доступом;

e) изменения или попытки изменить параметры настройки системы безопасности и мер и средств контроля и управления.

Как часто следует анализировать результаты мониторинга деятельности, должно зависеть от возможных рисков информационной безопасности. Подлежащие рассмотрению факторы риска включают в себя:

a) критичность процессов, которые поддерживаются прикладными программами;

b) ценность, чувствительность и критичность затрагиваемой информации;

c) предшествующий случай проникновения и неправильного использования системы, а также частота использования уязвимостей;

d) степень взаимосвязи систем (особенно с общедоступными сетями);

e) деактивацию средств регистрации.

Дополнительная информация

Процедуры мониторинга использования систем нужны для обеспечения уверенности в том, что пользователи выполняют только те действия, которые были явно разрешены.

Анализ журнала регистрации способствует пониманию угроз, с которыми сталкивается система, и каким образом они могут возникать. Примеры событий, для которых могло бы потребоваться дальнейшее расследование в случае инцидентов информационной безопасности, приведены в 13.1.1.

10.10.3 Защита информации журналов регистрации

Мера и средство контроля и управления

Средства регистрации и информацию журналов регистрации следует защищать от повреждения и неавторизованного доступа.

Рекомендация по реализации

Использование мер и средств контроля и управления должно быть нацелено на защиту от неавторизованных изменений и эксплуатационных проблем средств регистрации, включая:

a) изменения типов записываемых сообщений;

b) редактирование или удаление файлов журнала регистрации;

c) превышение объема памяти носителя, содержащего файл журнала регистрации, что может приводить либо к отказу регистрировать события, либо к затиранию[1)] информации о событиях, зарегистрированных в последнюю очередь.

Архивация некоторых контрольных журналов может требоваться как часть политики хранения записей или вследствие требований собирать и хранить доказательство (см. 13.2.3).

Дополнительная информация

Системные журналы часто содержат большой объем информации, значительная часть которой не представляет интереса с точки зрения мониторинга безопасности. Чтобы помочь в выявлении значимых событий в целях мониторинга безопасности, необходимо рассмотреть возможность автоматической записи соответствующих типов сообщений в отдельный журнал регистраций и (или) использования подходящих системных утилит или инструментальных средств аудита для осуществления контрольного считывания и оптимизации файла.

Системные журналы необходимо защищать, так как если данные в них модифицированы или удалены, то они могут создавать ложное чувство безопасности.

10.10.4 Журналы регистрации администратора и оператора

Мера и средство контроля и управления

Действия системного администратора и системного оператора следует регистрировать.

Рекомендация по реализации

Журналы регистрации должны содержать:

a) время, когда произошло событие (успешное или неуспешное);

b) информацию о событии (например обработанные файлы) или об отказе (например произошла ошибка и было предпринято корректирующее действие);

c) учетную запись и имя администратора или оператора, сделавшего ее;

d) перечень задействованных процессов.

Анализ журналов регистрации системного администратора и оператора следует проводить на регулярной основе.

Дополнительная информация

Система обнаружения вторжения, менеджмент которой осуществляется вне рамок контроля системных и сетевых администраторов, может быть использована для осуществления мониторинга действий системного и сетевого администрирования на предмет соответствия.

10.10.5 Регистрация неисправностей

Мера и средство контроля и управления

Неисправности следует регистрировать, анализировать, и предпринимать в их отношении необходимые действия.

Рекомендация по реализации

Неисправности, о которых стало известно от пользователей или посредством системных программ, имеющих отношение к проблемам, связанным с системами обработки информации или коммуникационными системами, необходимо регистрировать. Должны существовать четкие правила обработки неисправностей, включая:

a) анализ журналов регистрации неисправностей для обеспечения уверенности в том, что неисправности были соответствующим образом устранены;

b) анализ корректирующих мероприятий для обеспечения уверенности в том, что меры и средства контроля и управления не были скомпрометированы и что предпринятое действие полностью авторизовано.

Должна обеспечиваться уверенность в том, что регистрация ошибок становится возможной, если данная системная функция доступна.

Дополнительная информация

Регистрация ошибок и неисправностей может влиять на производительность системы. Разрешение на такую регистрацию следует давать компетентному персоналу, а уровень регистрации, требуемый для отдельных систем, должен определяться оценкой рисков, с учетом снижения производительности.

[1)] Запись поверх ранее записанной информации.

10.10.6 Синхронизация часов

Мера и средство контроля и управления

Часы во всех соответствующих системах обработки информации в пределах организации или домена безопасности должны быть синхронизированы с установленным источником точного времени.

Рекомендация по реализации

Если компьютер или устройство связи имеет возможность использовать часы, работающие в реальном времени, то эти часы должны быть установлены по согласованному нормативу, т. е. всемирного координированного времени или местного стандартного времени. Поскольку некоторые часы, как известно, со временем начинают «спешить» или «отставать», должна существовать процедура, которая выявляет и исправляет любые значимые отклонения.

Правильная интерпретация формата дата/время важна для обеспечения уверенности в том, что временна́я отметка отражает реальную дату/время. Необходимо учитывать местную специфику (например переход на «летнее время»).

Дополнительная информация

Правильная установка компьютерных часов важна для обеспечения точности данных в контрольных журналах, которые могут потребоваться для расследований или в качестве доказательства в правовых (судебных) или дисциплинарных административных делах. Неаккуратные контрольные журналы могут затруднять такие расследования и дискредитировать эти доказательства. Часы, настроенные в соответствии с сигналами национальных атомных часов, передаваемыми по радио, могут использоваться как главные часы для настройки систем регистрации. Протокол сетевого времени может использоваться для поддержания всех серверов в состоянии, синхронизированном с главными часами.

11 Управление доступом

11.1 Требование бизнеса по управлению доступом

Цель: Управлять доступом к информации.

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

Правила управления доступом должны учитывать политику в отношении распространения и авторизации информации.

11.1.1 Политика управления доступом

Мера и средство контроля и управления

Политика управления доступом должна создаваться, документально оформляться и пересматриваться с учетом требований бизнеса и безопасности для доступа.

Рекомендация по реализации

Правила управления доступом и права каждого пользователя или группы пользователей должны быть четко сформулированы в политике управления доступом. Существует как логическое, так и физическое управление доступом (см. 9), и их следует рассматривать совместно. Пользователям и поставщикам услуг должны быть представлены четко сформулированные требования бизнеса, предъявляемые к управлению доступом.

Необходимо, чтобы в политике было учтено следующее:

a) требования в отношении безопасности конкретных прикладных программ бизнеса;

b) определение всей информации, связанной с прикладными программами бизнеса, и рисков, касающихся информации;

c) правила в отношении распространения информации и авторизации доступа, например необходимо знать принципы и уровни безопасности и классификации информации (см. 7.2);

d) согласованность между управлением доступом и политиками классификации информации различных систем и сетей;

e) соответствующие требования законодательства и любые договорные обязательства в отношении защиты доступа к данным или услугам (см. 15.1);

f) стандартные профили доступа пользователей для должностных ролей в организации;

g) менеджмент прав доступа в распределенной среде или сетях с учетом всех типов доступных соединений;

h) разделение ролей в отношении управления доступом, например запрос доступа, авторизация доступа, администрирование доступа;

i) требования в отношении формального разрешения запросов доступа (см. 11.2.1);

j) требования в отношении периодического пересмотра управления доступом (см. 11.2.4);

k) аннулирование прав доступа (см. 8.3.3).

Дополнительная информация

При определении правил управления доступом, следует принимать во внимание следующее:

a) различие между правилами, обязательными для исполнения, и рекомендациями, которые являются необязательными или обусловленными чем-либо;

b) установление правил, основанных на предпосылке «все 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 информационных метках (см. 7.2), инициированных как автоматически средствами обработки информации, так и по усмотрению пользователя;

d) изменения в правах пользователя как устанавливаемые автоматически информационной системой, так и определенные администратором;

e) правила, которые требуют особого разрешения перед применением, а также те, которые не требуют разрешения.

Правила управления доступом должны поддерживаться формальными процедурами и четко определенными обязанностями (см., например 6.1.3, 11.3, 10.4.1, 11.6).

11.2 Менеджмент доступа пользователей

Цель: Обеспечить уверенность в том, что доступ предоставлен авторизованным пользователям и предотвращен неавторизованный доступ к информационным системам.

Необходимо наличие формальных процедур по контролю предоставления прав доступа к информационным системам и услугам.

Процедуры должны охватывать все стадии жизненного цикла доступа пользователей, от начальной регистрации новых пользователей до окончательной отмены регистрации пользователей, которым больше не требуется доступ к информационным системам и услугам. Особое внимание должно быть уделено, где это необходимо, контролю предоставления привилегированных прав доступа, которые позволяют пользователям изменять управление системой.

11.2.1 Регистрация пользователей

Мера и средство контроля и управления

Необходима формальная процедура регистрации и снятия с учета пользователей в отношении предоставления и отмены доступа ко всем информационным системам и услугам.

Рекомендация по реализации

Процедура управления доступом в отношении регистрации и снятия с учета пользователей должна включать:

a) использование уникальных идентификаторов пользователей, позволяющих отследить действия пользователей, чтобы они несли ответственность за свои действия; использование групповых идентификаторов следует разрешать только там, где это необходимо для бизнеса или по условиям эксплуатации, все это должно быть утверждено и документировано;

b) проверку того, что пользователь имеет разрешение владельца системы на использование информационной системы или услуги; наличие отдельного разрешения на право доступа от руководства также может быть уместным;

c) проверку того, что уровень предоставленного доступа соответствует целям бизнеса (см. 9.1) и согласуется с политикой безопасности организации, например не нарушает принципа разграничения обязанностей (см. 10.1.3);

d) предоставление пользователям письменного заявления об их правах доступа;

e) требование от пользователей подписать заявление о принятии условий доступа;

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

g) ведение формального учета всех лиц, зарегистрированных как пользователи услуг;

h) немедленную отмену или блокирование прав доступа пользователей, у которых изменились роль, или рабочее место, или уволившихся из организации;

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

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

Дополнительная информация

Необходимо рассмотреть возможность создания ролей доступа пользователей, основанных на требованиях бизнеса, которые объединяют несколько прав доступа в типовые профили доступа пользователей. Управление запросами и пересмотром предоставления прав доступа (см. 11.2.4) легче осуществлять на уровне таких ролей, чем на уровне отдельных прав.

Необходимо рассмотреть возможность включения положений о соответствующих санкциях в случае попыток неавторизованного доступа в трудовые договора сотрудников и договора о предоставлении услуг (см. 6.1.5, 8.1.3 и 8.2.3).

11.2.2 Управление привилегиями

Мера и средство контроля и управления

Предоставление и использование привилегий необходимо ограничивать и контролировать.

Рекомендация по реализации

Необходимо, чтобы в многопользовательских системах, которые требуют защиты от неавторизованного доступа, предоставление привилегий контролировалось посредством формального процесса авторизации. Необходимо рассмотреть следующие меры:

a) определение привилегий доступа в отношении каждого системного продукта, например эксплуатируемой системы, системы управления базами данных, каждой прикладной программы и пользователей, которым эти привилегии должны быть предоставлены;

b) привилегии должны предоставляться пользователям на основании принципа необходимости и принципа «событие за событием» в соответствии с политикой управления доступом (см. 11.1.1), т. е. минимального требования для их функциональной роли, только при необходимости;

c) обеспечение процесса авторизации и регистрации в отношении всех предоставленных привилегий, привилегии не должны предоставляться до завершения процесса авторизации;

d) проведение политики разработки и использования стандартных системных утилит (скриптов), для того чтобы избежать необходимости предоставления привилегий пользователям;

e) поощрение разработки и использования программ, позволяющих избежать необходимости предоставления привилегий при их исполнении;

f) использование различных идентификаторов пользователей при работе в нормальном режиме и с использованием привилегий.

Дополнительная информация

Неадекватное использование привилегий в отношении администрирования системы (любой возможности или средства информационной системы, которые позволяют пользователю обходить меры и средства контроля и управления системы или прикладных программ) может быть одной из главных причин отказа или нарушения работы систем.

11.2.3 Управление паролями пользователей

Мера и средство контроля и управления

Распределение паролей необходимо контролировать посредством формального процесса управления.

Рекомендация по реализации

Процесс должен включать следующие требования:

a) пользователей необходимо обязать подписать заявление о сохранении личных паролей в тайне и сохранении групповых паролей исключительно в пределах членов данной группы; это заявление может быть включено в условия и положения занятости (см. 8.1.3);

b) если пользователи самостоятельно управляют собственными паролями, им следует первоначально предоставить безопасный вре́менный пароль (см. 11.3.1), который подлежит немедленной принудительной замене после входа в систему;

c) создание процедур проверки личности пользователя, прежде чем ему будет предоставлен новый, заменяющий или временный пароль;

d) временные пароли следует выдавать пользователям безопасным способом, при этом необходимо избегать использования третьих сторон или незащищенного (открытого) текста сообщений электронной почты;

e) временные пароли должны быть уникальны для каждого пользователя и не должны быть легко угадываемыми;

f) пользователи должны подтверждать получение паролей;

g) пароли никогда не следует хранить в компьютерных системах в незащищенной форме;

h) пароли поставщика, установленные по умолчанию, необходимо изменить после инсталляции систем или программного обеспечения.

Дополнительная информация

Пароли являются распространенным средством подтверждения личности пользователя перед предоставлением ему доступа к информационной системе или услуге в соответствии с его авторизацией. При необходимости следует рассмотреть возможность использования других технологий для идентификации и аутентификации пользователей, таких как биометрия, например проверка отпечатков пальцев, проверка подписи, а также использование аппаратных средств идентификации, например смарт-карт.

11.2.4 Пересмотр прав доступа пользователей

Мера и средство контроля и управления

Руководство должно осуществлять формальный процесс периодического пересмотра прав доступа пользователей.

Рекомендация по реализации

При пересмотре прав доступа должны учитываться следующие рекомендации:

a) права доступа должны пересматриваться регулярно, например через шесть месяцев, и после любых изменений, таких как повышение/понижение в должности, или увольнения (см. 11.2.1);

b) права доступа пользователей должны пересматриваться и переназначаться при переходе с одной работы на другую в пределах одной организации;

c) разрешения в отношении специальных привилегированных прав доступа (см. 11.2.2) должны пересматриваться через небольшие интервалы времени, например через три месяца;

d) предоставленные привилегии должны пересматриваться через равные интервалы времени для обеспечения уверенности в том, что не были получены неавторизованные привилегии;

e) изменения привилегированных учетных записей должны регистрироваться для периодического анализа.

Дополнительная информация

С целью поддержания эффективного контроля над доступом к данным и информационным услугам необходимо регулярно пересматривать права доступа пользователей.

11.3 Обязанности пользователя

Цель: Предотвращение неавторизованного доступа пользователей, а также компрометации или кражи информации и средств обработки информации.

Сотрудничество авторизованных пользователей – важный аспект эффективной безопасности.

Пользователи должны быть осведомлены о своих обязанностях в отношении поддержания эффективного управления доступом, в частности, в отношении паролей и безопасности оборудования, с которым они работают.

Следует внедрять политику «чистого стола» и «чистого экрана» в целях снижения риска неавторизованного доступа или повреждения бумажных документов, носителей информации и средств обработки информации.

11.3.1 Использование паролей

Мера и средство контроля и управления

Пользователи должны придерживаться общепринятой практики в области безопасности при выборе и использовании паролей.

Рекомендация по реализации

Всем пользователям следует рекомендовать:

a) сохранять конфиденциальность паролей;

b) избегать записи паролей (например на бумаге, в файле программного обеспечения или карманных устройствах), если не может быть обеспечено безопасное хранение и способ хранения не утвержден;

c) изменять пароли всякий раз, когда появляется любой признак возможной компрометации системы или пароля;

d) выбирать качественные пароли с достаточно минимальной длиной, которые:

1) легко запомнить;

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

3) не могут быть восстановлены по словарям (т. е., не содержат слов, содержащихся в словарях);

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

e) изменять пароли через разные интервалы времени или после определенного числа обращений к системе (пароли для привилегированных учетных записей следует менять чаще, чем обычные пароли) и избегать повторного или циклического использования старых паролей;

f) изменять временные пароли при первом начале сеанса;

g) не включать пароли ни в какой автоматизированный процесс начала сеанса, например с использованием хранимых макрокоманд или функциональных клавиш;

h) не использовать коллективно индивидуальные пользовательские пароли;

i) не использовать один и тот же пароль для бизнеса и некомерческих целей.

Если пользователи нуждаются в доступе к многочисленным услугам, системам или платформам и вынуждены использовать несколько разных паролей, они должны знать, что могут использовать единый качественный пароль (см. перечисление d) 11.3.1) для всех услуг при уверенности, что разумный уровень защиты для хранения пароля был создан в рамках каждой услуги, системы или платформы.

Дополнительная информация

Особую осторожность следует соблюдать при менеджменте системы «справочного стола», имеющей дело с утерянными или забытыми паролями, поскольку это может быть средством атаки на систему паролей.

11.3.2 Оборудование пользователя, оставленное без присмотра

Мера и средство контроля и управления

Пользователи должны обеспечивать соответствующую защиту оборудования, оставленного без присмотра

Рекомендация по реализации

Всем пользователям необходимо знать требования безопасности и процедуры в отношении защиты оставленного без присмотра оборудования, а также их обязанности по обеспечению такой защиты. Пользователям рекомендуется:

a) завершать активные сеансы по окончании работы, если отсутствует соответствующий механизм блокировки, например защищенная паролем экранная заставка;

b) завершить сеанс на системах мэйнфреймов, серверах и офисных персональных компьютерах, когда работа завершена (т. е. не только выключить экран персонального компьютера или терминал);

c) обеспечивать безопасность персональных компьютеров или терминалов от несанкционированного использования с помощью блокировки клавиатуры или эквивалентных средств контроля, например доступа по паролю, когда оборудование не используется (см. 11.3.3).

Дополнительная информация

Оборудование, установленное в пользовательских зонах, например рабочие станции или файловые серверы, может потребовать специальной защиты от несанкционированного доступа, если оно оставлено без присмотра на длительный период.

11.3.3 Политика «чистого стола» и «чистого экрана»

Мера и средство контроля и управления

Необходимо принять политику «чистого стола» в отношении бумажных документов и сменных носителей данных, а также политику «чистого экрана» в отношении средств обработки информации.

Рекомендация по реализации

Политика «чистого стола» и «чистого экрана» должна учитывать классификацию информации (см. 7.2), законодательные и договорные требования (см. 15.1), а также соответствующие риски и корпоративную культуру организации. Необходимо рассмотреть следующие рекомендации:

a) носители (бумажные или электронные), содержащие чувствительную или критическую информацию бизнеса, когда они не используются, следует убирать и запирать (лучше всего, в несгораемый сейф или шкаф), особенно, когда помещение пустует;

b) компьютеры и терминалы, когда их оставляют без присмотра, следует выключать или защищать посредством механизма блокировки экрана или клавиатуры, контролируемого паролем, токеном или аналогичным механизмом аутентификации пользователя, а также необходимо применять кодовые замки, пароли или другие меры и средства контроля и управления в то время, когда эти устройства не используются;

c) необходимо обеспечить защиту пунктов приема/отправки корреспонденции, а также автоматических факсимильных аппаратов;

d) необходимо предотвращать несанкционированное использование фотокопировальных устройств и другой воспроизводящей техники (сканеров, цифровых фотоаппаратов);

e) документы, содержащие чувствительную или критическую информацию, необходимо немедленно изымать из принтеров.

Дополнительная информация

Политика «чистого стола»/«чистого экрана» снижает риски несанкционированного доступа, потери и повреждения информации как во время рабочего дня, так и вне рабочего времени. Сейфы или другие формы средств безопасного хранения также могут защищать хранимую в них информацию от форс-мажорных обстоятельств, таких как пожар, землетрясение, наводнение или взрыв.

Стоит обратить внимание на использование принтеров с функцией ПИН-кода, тогда только инициаторы отправления на печать смогут получать свои распечатки, и только если они стоят рядом с принтером.

11.4 Управление доступом к сети

Цель: Предотвратить неавторизованный доступ к сетевым услугам.

Доступ к внутренним и внешним сетевым услугам должен быть контролируемым.

Это необходимо для получения уверенности в том, что пользователи, которые имеют доступ к сетям и сетевым услугам, не нарушают их безопасность, путем:

a) обеспечения соответствующих интерфейсов между сетью организации и сетями, принадлежащими другим организациям, и общедоступными сетями;

b) внедрения соответствующих механизмов аутентификации в отношении пользователей и оборудования;

c) предписанного управления доступом пользователей к информационным услугам.

11.4.1 Политика использования сетевых услуг

Мера и средство контроля и управления

Пользователям следует предоставлять доступ только к тем услугам, на использование которых они были специально уполномочены.

Рекомендация по реализации

Следует сформулировать политику относительно использования сетей и сетевых услуг.

В политике необходимо рассмотреть:

a) сети и сетевые услуги, к которым разрешен доступ;

b) процедуры авторизации для определения того, кому и к каким сетям и сетевым услугам разрешен доступ;

c) меры и средства контроля и управления, а также процедуры менеджмента по защите доступа к сетевым подключениям и сетевым услугам;

d) средства, используемые для осуществления доступа к сетям и сетевым услугам (например условия, обеспечивающие возможность доступа по коммутируемой телефонной линии к провайдеру Интернет-услуг или удаленной системе).

Политика использования сетевых услуг должна быть согласована с политикой управления доступом (см. 11.1).

Дополнительная информация

Несанкционированные и незащищенные подключения к сетевым услугам могут затрагивать целую организацию. Мера и средство контроля и управления, в частности, важна для сетевых подключений к чувствительным или критическим прикладным программам бизнеса, или в отношении пользователей, находящихся в зонах высокого риска, например в общественных местах или за пределами организации, т. е. в общественных или внешних зонах, которые находятся за пределами непосредственного управления и контроля безопасностью со стороны организации.

11.4.2 Аутентификация пользователей для внешних соединений

Мера и средство контроля и управления

Для управления доступом удаленных пользователей следует применять соответствующие методы аутентификации.

Рекомендация по реализации

Аутентификация удаленных пользователей может быть достигнута при использовании, например методов, основанных на применении средств криптографии, аппаратных средств защиты (токенов) или протоколов «запрос-ответ». Примером возможной реализации таких методов могут служить различные решения в отношении виртуальных частных сетей. Выделенные частные линии могут также использоваться для обеспечения доверия к источнику подключений.

Процедуры, меры и средства контроля и управления обратного вызова, например использование модемов с обратным вызовом, могут обеспечить защиту от несанкционированных и нежелательных подключений к средствам обработки информации организации. Указанные меры позволяют произвести аутентификацию пользователей, пытающихся установить удаленную связь с сетью организации. При использовании данной меры и средства контроля и управления организации не следует применять сетевые сервисы, которые включают переадресацию вызова, или, если они это делают, то они должны отключить использование таких функций, чтобы избежать недостатков, связанных с переадресацией вызова. Процесс обратного вызова должен обеспечить уверенность в том, что фактическое разъединение происходит на стороне организации. В противном случае, удаленный пользователь может держать линию открытой, считая, что произошла проверка обратного вызова. Процедуры, меры и средства контроля и управления обратного вызова следует тщательного протестировать на предмет наличия такой возможности.

Аутентификация узла может служить альтернативным средством аутентификации групп удаленных пользователей там, где они подсоединены к безопасному компьютерному средству совместного использования. Для аутентификации узла могут применяться криптографические методы, основанные, например, на механизме сертификации. Это является частью некоторых решений, основанных на виртуальных частных сетях.

Должны быть реализованы дополнительные меры и средства контроля и управления аутентификацией для управления доступом к беспроводным сетям. В частности, необходимо проявлять особую осторожность при выборе мер и средств контроля и управления для беспроводных сетей по причине больших возможностей необнаруживаемого перехвата и ввода сетевого трафика.

Дополнительная информация

Внешние соединения обеспечивают благоприятную возможность для несанкционированного доступа к информации бизнеса, например доступа с использованием методов соединения по телефонной линии. Существуют различные методы аутентификации, некоторые из которых обеспечивают больший уровень защиты, чем другие, например методы, основанные на использовании средств криптографии, могут обеспечить достаточно надежную защиту. Исходя из оценки риска, важно определить требуемый уровень защиты. Это необходимо для соответствующего выбора метода аутентификации.

Наличие возможности автоматического подсоединения к удаленному компьютеру — это один из способов получения несанкционированного доступа к прикладной программе бизнеса. Это особенно важно, если для подсоединения используется сеть, которая находится вне сферы контроля менеджмента безопасности организации.

11.4.3 Идентификация оборудования в сетях

Мера и средство контроля и управления

Автоматическую идентификацию оборудования необходимо рассматривать как средство для аутентификации подсоединений, осуществляемых с определенных мест или определенного оборудования.

Рекомендация по реализации

Идентификацию оборудования можно применять в тех случаях, когда важно, чтобы связь могла быть инициирована только с определенного места или оборудования. Для того чтобы показать, разрешено ли этому оборудованию подсоединение к сети, может быть использован внутренний или прикрепленный к оборудованию идентификатор. Такие идентификаторы должны четко показывать, к какой сети разрешено подключать оборудование, если эта сеть не единственная и, особенно, если эти сети имеют разную степень чувствительности. Для обеспечения безопасности идентификатора оборудования может возникнуть необходимость физической защиты оборудования.

Дополнительная информация

Эти меры и средства контроля и управления могут быть дополнены другими методами, направленными на аутентификацию пользователя оборудования (см. 11.4.2). Идентификация оборудования может применяться дополнительно к аутентификации пользователя.

11.4.4 Защита портов дистанционной диагностики и конфигурации

Мера и средство контроля и управления

Физический и логический доступ для портов дистанционной диагностики и конфигурации должен быть контролируемым и управляемым.

Рекомендация по реализации

Возможные меры и средства контроля и управления доступом к портам дистанционной диагностики и конфигурации включают в себя использование блокировки клавиш и поддерживающих процедур для контроля физического доступа к порту. Примером такой поддерживающей процедуры является обеспечение

уверенности в том, что доступ к портам дистанционной диагностики и конфигурации осуществляется только при условии взаимной договоренности между руководителем, отвечающим за предоставление компьютерных услуг, и персоналом по поддержке аппаратных/программных средств.

Порты, сервисы и аналогичные средства, установленные на компьютере или сетевом оборудовании, которые определенно не требуются для функциональности бизнеса, следует блокировать или удалять.

Дополнительная информация

Многие компьютерные системы, сетевые системы и системы связи внедряются со средствами удаленной диагностики или конфигурации для использования инженерами по обслуживанию. Будучи незащищенными, эти диагностические порты предоставляют возможность неавторизованного доступа.

11.4.5 Разделение в сетях

Мера и средство контроля и управления

Группы информационных услуг, пользователей и информационных систем в пределах сети должны быть разделены.

Рекомендация по реализации

Один из методов контроля безопасности больших сетей состоит в том, чтобы разделить их на отдельные логические сетевые домены, например на внутренние сетевые домены организации и внешние сетевые домены, каждый из которых защищен определенным периметром безопасности. Совокупность последовательных мер и средств контроля и управления может быть применена в различных логических сетевых доменах для дальнейшего разделения среды сетевой безопасности, например общедоступные системы, внутренние сети и критические активы. Домены должны определяться на основе оценки риска и различных требований в отношении безопасности в пределах каждого из доменов.

Такой сетевой периметр может быть реализован посредством внедрения шлюза безопасности между двумя связанными сетями для управления доступом и информационным потоком между двумя доменами. Данный шлюз следует конфигурировать для фильтрации трафика между доменами (см. 11.4.6 и 11.4.7) и для блокирования несанкционированного доступа в соответствии с политикой организации по управлению доступом (см. 11.1). Примером шлюза такого типа является межсетевой экран. Другим методом разделения отдельных логических доменов является ограничение сетевого доступа при использовании виртуальных частных сетей для групп пользователей в пределах организации.

Сети также могут быть разделены с помощью функциональных возможностей сетевых устройств, например IP-коммутации[1)]. Отдельные домены могут быть, кроме того, реализованы посредством управления потоками сетевых данных при использовании возможностей маршрутизации/коммутации, например списков управления доступом.

Критерии для разделения сетей на домены следует основывать на политике управления доступом и требованиях к доступу (см. 10.1) с учетом влияния на относительную стоимость и производительность включения соответствующей технологии маршрутизации сетей и шлюзов (см. 11.4.6 и 11.4.7).

Кроме того, разделение сетей должно основываться на ценности и классификации информации, хранимой или обрабатываемой в сети, уровнях доверия или сферах деятельности, для того чтобы снизить последствия от прерывания услуг.

Следует уделять внимание отделению беспроводных сетей от внутренних и частных сетей. Поскольку периметры беспроводных сетей не являются достаточно определенными, следует проводить оценку риска, чтобы идентифицировать меры и средства контроля и управления (например строгую аутентификацию, криптографические методы и выбор частоты) для поддержки разделения сетей.

Дополнительная информация

Сети все более распространяются за традиционные границы организации, поскольку создаются деловые партнерства, которые могут потребовать коммуникаций или совместного использования сетевой инфраструктуры и средств обработки информации. Такие расширения могут увеличить риск несанкционированного доступа к существующим информационным системам, которые используют сеть, причем в отношении некоторых из этих систем, вследствие их чувствительности или критичности, может потребоваться защита от других пользователей, получивших доступ к сети.

11.4.6 Управление сетевыми соединениями

Мера и средство контроля и управления

Присоединение пользователей к совместно используемым сетям, особенно тем, которые выходят за рамки организации, необходимо ограничивать в соответствии с политикой управления доступом и требованиями прикладных программ бизнеса (см. 11.1).

[1)] IP — протокол межсетевого взаимодействия (базовый интернет-протокол).

Рекомендация по реализации

Права пользователей в отношении сетевого доступа должны поддерживаться и обновляться в соответствии с требованиями политики управления доступом (см. 11.1.1).

Возможность подсоединения пользователей может ограничиваться сетевыми шлюзами, фильтрующими трафик посредством предварительно определенных таблиц или правил. Примерами прикладных программ, к которым следует применить ограничения являются:

a) обмен сообщениями, например электронная почта;

b) передача файлов;

c) интерактивный доступ;

d) доступ к прикладной программе.

Следует рассмотреть права доступа к сети, приуроченные к определенному времени суток или дате.

Дополнительная информация

Требования политики управления доступом для совместно используемых сетей, особенно тех, которые выходят за рамки организации, могут вызвать необходимость внедрения дополнительных мер и средств контроля и управления, чтобы ограничить возможности пользователей по подсоединению.

11.4.7 Управление сетевой маршрутизацией

Мера и средство контроля и управления

Для сетей следует внедрять меры и средства контроля и управления маршрутизацией, чтобы обеспечить уверенность в том, что подсоединения компьютеров и информационные потоки не нарушают политику управления доступом к прикладным программам бизнеса.

Рекомендация по реализации

Необходимо, чтобы меры и средства контроля и управления маршрутизацией основывались на механизмах проверки реальных адресов источника и получателя.

Шлюзы безопасности могут использоваться для подтверждения адресов источника и получателя на внутренней и внешней точках управления сетью, если используются технологии трансляции сетевых адресов и (или) прокси-сервер. Необходимо, чтобы специалисты, занимающиеся внедрением, были осведомлены о преимуществах и недостатках различных используемых механизмов. Требования в отношении мер и средств контроля и управления маршрутизацией сети должны основываться на политике управления доступом (см. 11.1).

Дополнительная информация

Сети совместного использования, особенно те, которые выходят за рамки организации, могут потребовать внедрения дополнительных мер и средств контроля и управления маршрутизацией. Это, особенно, касается сетей, используемых совместно с пользователями третьей стороны (не организации).

11.5 Управление доступом к эксплуатируемой системе

Цель: Предотвратить несанкционированный доступ к эксплуатируемым системам.

Средства безопасности следует использовать, для того чтобы возможность осуществления доступа предоставлялась только авторизованным пользователям. Необходимо, чтобы данные средства могли обеспечить следующее:

a) аутентификацию авторизованных пользователей в соответствии с определенной политикой управления доступом;

b) регистрацию успешных и неудавшихся попыток аутентификации для осуществления доступа к системе;

c) регистрацию использования специальных системных привилегий;

d) срабатывание сигнализации при нарушении политик безопасности системы;

e) обеспечение соответствующих средств для аутентификации;

f) при необходимости, ограничение времени подсоединения пользователей.

11.5.1 Безопасные процедуры начала сеанса

Мера и средство контроля и управления

Доступ к эксплуатируемым системам должен контролироваться посредством безопасной процедуры начала сеанса.

Рекомендация по реализации

Процедура регистрации в эксплуатируемой системе должна быть спроектирована так, чтобы свести к минимуму возможность несанкционированного доступа. Поэтому необходимо, чтобы процедура начала сеанса раскрывала минимум информации о системе, во избежание оказания какой-либо ненужной

помощи неавторизованному пользователю. Правильная процедура начала сеанса характеризуется следующими свойствами:

a) не отображает наименований системы или прикладных программ, пока процесс начала сеанса не будет успешно завершен;

b) отображает общее предупреждение о том, что доступ к компьютеру могут получить только авторизованные пользователи;

c) не предоставляет сообщений-подсказок в течение процедуры начала сеанса, которые могли бы помочь неавторизованному пользователю;

d) подтверждает информацию начала сеанса только по завершении ввода всех исходных данных, в случае ошибочного ввода, система не должна показывать, какая часть данных является правильной или неправильной;

e) ограничивает число разрешенных неудачных попыток начала сеанса (например три попытки) и предусматривает:

1) протоколирование неудачных и удачных попыток;

2) включение временной задержки прежде, чем будут разрешены дальнейшие попытки начала сеанса, или отклонение любых дальнейших попыток без специальной авторизации;

3) разъединение сеанса связи и передачи данных;

4) отправление предупредительного сообщения на системный пульт, если достигнуто максимальное число попыток начала сеанса;

5) установление числа повторного ввода паролей с учетом минимальной длины пароля и значимости защищаемой системы;

f) ограничивает максимальное и минимальное время, разрешенное для процедуры начала сеанса, если оно превышено, система должна прекратить начало сеанса;

g) отображает следующую информацию в отношении успешного завершения начала сеанса:

1) дату и время предыдущего успешного начала сеанса;

2) подробную информацию о любых неудачных попытках начала сеанса, начиная с последнего успешного начала сеанса;

h) не отображает введенный пароль или предусматривает скрытие знаков пароля с помощью символов;

i) не передает пароли открытым текстом по сети.

Дополнительная информация

Если пароли передаются в открытом виде по сети в течение начала сеанса сессии, они могут быть перехвачены в сети программой сетевого «сниффера»[1)].

11.5.2 Идентификация и аутентификация пользователя

Мера и средство контроля и управления

Необходимо, чтобы все пользователи имели уникальный идентификатор (идентификатор пользователя), предназначенный только для их личного использования, и должен быть выбран подходящий способ проверки для подтверждения заявленной подлинности пользователя.

Рекомендация по реализации

Меры и средства контроля и управления должна применяться в отношении всех типов пользователей (включая персонал технической поддержки, операторов, администраторов сети, системных программистов и администраторов баз данных).

Идентификаторы пользователей необходимо использовать для отслеживания действий подотчетного лица. Регулярные действия пользователей не должны выполняться из привилегированных учетных записей.

При исключительных обстоятельствах, когда имеется очевидная выгода для бизнеса, может использоваться общий идентификатор для группы пользователей или для выполнения определенной работы. В таких случаях необходимо документально оформлять разрешение руководства. Могут потребоваться дополнительные меры и средства контроля и управления для поддержания отслеживаемости.

Разрешение на индивидуальное использование группового идентификатора следует давать только тогда, когда функции общедоступны, или нет необходимости отслеживать действия, выполняемые с помощью данного идентификатора (например доступ только для чтения), или когда применяются другие меры контроля (например пароль для группового идентификатора выдается единовременно только для одного сотрудника и такой случай регистрируется).

[1)] Программа для «прослушивания» сетевого соединения на уровне пакетов.

Там, где требуются надежная аутентификация и идентификация личности, следует использовать аутентификационные методы, альтернативные по отношению к паролям, такие как криптографические средства, смарт-карты, токены или биометрические средства.

Дополнительная информация

Пароли (см. 11.3.1 и 11.5.3) являются очень распространенным способом обеспечения идентификации и аутентификации, основанным на тайне, которую знает только пользователь. Того же результата можно достигнуть средствами криптографии и аутентификационными протоколами. Надежность идентификации и аутентификации пользователя должна соответствовать чувствительности информации, к которой нужно осуществлять доступ.

Такие объекты как токены с памятью или смарт-карты, которыми обладают пользователи, также могут применяться для идентификации и аутентификации. Биометрические технологии аутентификации, которые используют уникальные характеристики или особенности индивидуума, также могут служить для подтверждения подлинности личности. Сочетание различных технологий и механизмов, связанных безопасным способом, обеспечивает более надежную аутентификацию.

11.5.3 Система управления паролями

Мера и средство контроля и управления

Системы управления паролями должны быть интерактивными и должны обеспечивать уверенность в качестве паролей.

Рекомендация по реализации

Система управления паролями должна:

a) предписывать использование индивидуальных пользовательских идентификаторов и паролей с целью установления персональной ответственности;

b) позволять пользователям выбирать и изменять свои пароли, и включать процедуру подтверждения ошибок ввода;

c) предписывать использование качественных паролей (см. 11.3.1);

d) принуждать к изменению паролей (см. 11.3.1);

e) заставлять пользователей изменять временные пароли при первом начале сеанса (см. 11.2.3);

f) вести учет 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 защищенной (например зашифрованной или хешированной) форме.

Дополнительная информация

Пароли являются одним из главных средств подтверждения полномочий пользователя, осуществляющего доступ к сервисам компьютера.

Некоторые прикладные программы требуют, чтобы пользовательские пароли назначались независимым органом; в таких случаях перечисления b), d) и e) приведенных выше рекомендаций не применяются. В большинстве же случаев, пароли выбираются и поддерживаются пользователями. Смотрите рекомендации по использованию паролей в 11.3.1.

11.5.4 Использование системных утилит

Мера и средство контроля и управления

Использование утилит, которые могли бы обойти меры и средства контроля и управления эксплуатируемых систем и прикладных программ, следует ограничивать и строго контролировать.

Рекомендация по реализации

Необходимо рассмотреть следующие рекомендации по использованию системных утилит:

a) использование процедур идентификации, аутентификации и авторизации для системных утилит;

b) отделение системных утилит от прикладных программ;

c) ограничение использования системных утилит минимальным числом доверенных авторизованных пользователей (см. 11.2.2);

d) авторизация на использование специальных системных утилит;

e) ограничение доступности системных утилит, например на время внесения авторизованных изменений;

f) регистрация использования всех системных утилит;

g) определение и документальное оформление уровней авторизации в отношении системных утилит;

h) удаление или блокирование ненужного программного обеспечения утилит и системного программного обеспечения;

i) обеспечение недоступности системных утилит для пользователей, имеющих доступ к прикладным программам на системах, где требуется разделение обязанностей.

Дополнительная информация

На большинстве компьютеров, как правило, установлена, одна или несколько системных обслуживающих программ (утилит), которые позволяют обойти меры и средства контроля и управления эксплуатируемых систем и прикладных программ.

11.5.5 Лимит времени сеанса связи

Мера и средство контроля и управления

Неактивные сеансы должны быть закрыты после определенного периода бездействия.

Рекомендация по реализации

Необходимо, чтобы механизм блокировки по времени обеспечивал очистку окна сеанса, а также, возможно позднее, после определенного периода бездействия закрывал прикладную программу и сетевые сеансы. Задержка, связанная с блокировкой по времени, должна отражать риски безопасности этой области, классификацию обрабатываемой информации и используемых прикладных программ, а также риски, связанные с пользователями оборудования.

Для некоторых систем может быть предусмотрена ограниченная форма средств блокировки по времени, которая очищает экран и предотвращает неавторизованный доступ, но не закрывает прикладные программы или сетевые сеансы.

Дополнительная информация

Данная мера и средство контроля и управления особенно важна в местах повышенного риска, например в общедоступных местах или на внешней территории, находящейся вне сферы действия менеджмента безопасности организации. Для предотвращения доступа неавторизованных лиц и атак типа «отказ в обслуживании» сеансы необходимо закрывать.

11.5.6 Ограничения времени соединения

Мера и средство контроля и управления

Ограничения на время соединения должны быть использованы для обеспечения дополнительной безопасности прикладных программ с высокой степенью риска.

Рекомендация по реализации

Необходимо рассмотреть меры и средства контроля и управления в отношении времени подсоединения для чувствительных компьютерных приложений, особенно в местах повышенного риска, например общедоступных местах или на внешней территории, находящейся вне сферы действия менеджмента безопасности организации. Примерами таких ограничений являются:

a) использование заранее определенных отрезков времени, например для пакетной передачи файлов или регулярных интерактивных сеансов небольшой продолжительности;

b) ограничение времени подключения нормальными часами работы организации, если нет необходимости в сверхурочной или более продолжительной работе;

c) проведение повторной аутентификации через запланированные интервалы времени.

Дополнительная информация

Ограничение периода, в течение которого разрешены подсоединения к компьютерным сервисам, уменьшает интервал времени, в течение которого существует риск неавторизованного доступа. Ограничение продолжительности активных сеансов не позволяет пользователям держать сеансы открытыми, чтобы предотвратить повторную аутентификацию.

11.6 Управление доступом к информации и прикладным программам

Цель: Предотвратить неавторизованный доступ к информации прикладных систем.

Необходимо использовать средства безопасности для ограничения доступа к прикладным системам и внутри данных систем.

Круг лиц, имеющих логический доступ к прикладному программному обеспечению и информации, должен быть ограничен только авторизованными пользователями. Необходимо, чтобы прикладные системы обеспечивали следующее:

a) управление доступом пользователей к информации и функциям прикладных систем в соответствии с определенной политикой управления доступом;

b) защиту от неавторизованного доступа любой утилиты, программного обеспечения эксплуатируемой системы и вредоносной программы, которые позволяют отменять или обходить меры и средства контроля и управления системы или прикладных программ;

c) не представляли угрозу безопасности другим системам, совместно с которыми используются информационные ресурсы.

11.6.1 Ограничение доступа к информации

Мера и средство контроля и управления

Доступ пользователей и персонала поддержки к информации и функциям прикладных систем должен ограничиваться в соответствии с определенной политикой в отношении управления доступом.

Рекомендация по реализации

Ограничения доступа должны основываться на требованиях в отношении отдельных прикладных программ бизнеса. Политика управления доступом должна соответствовать политике доступа организации (см. 11.1).

Необходимо рассмотреть возможность применения следующих рекомендаций для соблюдения требований по ограничению доступа:

a) наличие пунктов меню, позволяющих управлять доступом к функциям прикладных систем;

b) управление правами доступа пользователей, например чтение, запись, удаление, выполнение;

c) управление правами доступа других прикладных программ;

d) обеспечение уверенности в том, что данные, выводимые из прикладных систем, обрабатывающих чувствительную информацию, содержат только требуемую информацию и отправлены только в адреса авторизованных терминалов и мест назначения; необходим периодический анализ процесса вывода для обеспечения уверенности в том, что избыточная информация удалена.

11.6.2 Изоляция чувствительных систем

Мера и средство контроля и управления

Чувствительные системы должны иметь специализированную (изолированную) вычислительную среду.

Рекомендация по реализации

В отношении систем, обрабатывающих чувствительную информацию, необходимо рассмотреть следующее:

a) владелец прикладной программы должен определить и документально оформить степень чувствительности данной прикладной программы (см. 7.1.2);

b) если чувствительная прикладная программа должна работать в среде совместного использования, владельцем данной прикладной программы должны быть выявлены другие прикладные программы, с которыми будут совместно использоваться ресурсы, а также идентифицированы и приняты соответствующие риски.

Дополнительная информация

Некоторые прикладные программы системы достаточно чувствительны к потенциальному ущербу и поэтому требуют особой эксплуатации. Чувствительность может указывать, что прикладная программа система:

a) должна работать на выделенном компьютере;

b) должна разделять ресурсы только с доверенными прикладными программами системы.

Изоляция может быть достигнута при использовании физических или логических методов (см. 11.4.5).

11.7 Мобильная вычислительная техника и дистанционная работа

Цель: Обеспечить уверенность в информационной безопасности при использовании средств мобильной вычислительной техники и дистанционной работы.

Следует соизмерять требуемую защиту со специфичными рисками работы в удаленном режиме. При использовании мобильной вычислительной техники следует учитывать риски, связанные с работой в незащищенной среде, и применять соответствующие средства защиты. В случаях дистанционной работы организации следует предусмотреть защиту мест дистанционной работы и обеспечить уверенность в соответствующей организации подобного способа работы.

11.7.1 Мобильная вычислительная техника и связь

Мера и средство контроля и управления

Необходимо принять формальную политику и обеспечить соответствующие меры безопасности для защиты от рисков, связанных с работой со средствами мобильной вычислительной техники и связи.

Рекомендация по реализации

При использовании мобильных вычислительных средств и средств связи, например ноутбуков, карманных компьютеров, лэптопов, смарт-карт и мобильных телефонов, необходимо принимать специальные меры для обеспечения уверенности в том, что бизнес-информация не скомпрометирована. Политика использования мобильных вычислительных средств должна учитывать риски, связанные с работой с переносными устройствами в незащищенной среде.

Политика использования мобильных вычислительных средств должна включать требования к физической защите, управлению доступом, использованию средств криптографии, резервирования и защиты от вирусов. Такая политика должна также включать правила и рекомендации относительно подсоединения мобильных средств к сетям, а также руководство по использованию этих средств в общедоступных местах.

Следует проявлять осторожность при использовании мобильных вычислительных средств в общедоступных местах, конференц-залах и других незащищенных местах вне организации. Необходимо обеспечить защиту от неавторизованного доступа или раскрытия информации, хранимой и обрабатываемой этими средствами, например с помощью средств криптографии (см. 12.3).

Важно при использовании мобильных вычислительных средств в общедоступных местах проявлять осторожность, во избежание риска вмешательства неавторизованных лиц. Необходимо внедрить и поддерживать в актуальном состоянии процедуры защиты от вредоносной программы (см. 10.4).

Необходимо регулярно делать резервные копии критической информации бизнеса. Следует также обеспечить доступность оборудования для быстрого и удобного резервного копирования информации. В отношении резервных копий необходимо обеспечить адекватную защиту, например от кражи или потери информации.

Соответствующую защиту необходимо обеспечить в отношении использования мобильных средств, подсоединенных к сетям. Удаленный доступ к информации бизнеса через общедоступную сеть с использованием мобильных средств вычислительной техники следует осуществлять только после успешной идентификации и аутентификации, а также при условии внедрения соответствующих механизмов управления доступом (см. 11.4).

Мобильные вычислительные средства 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. Для случаев потери или кражи мобильных вычислительных средств должна быть установлена специальная процедура, учитывающая законодательные, страховые и другие требования безопасности организации. Оборудование, в котором переносится важная, чувствительная и (или) критическая информация бизнеса, не следует оставлять без присмотра и по возможности должно быть физически заблокировано или должны быть использованы специальные замки для обеспечения безопасности оборудования (см. 9.2.5).

Необходимо провести тренинг сотрудников, использующих мобильные вычислительные средства, с целью повышения осведомленности о дополнительных рисках, связанных с таким способом работы и мерах и средствах контроля и управления, которые должны быть выполнены.

Дополнительная информация

Беспроводные подсоединения к сети мобильной связи аналогичны другим типам подсоединения к сети, однако они имеют важные отличия, которые необходимо учитывать при определении мер и средств контроля и управления. Типичными отличиями являются:

a) некоторые беспроводные небезупречные протоколы безопасности;

b) невозможность резервного копирования информации в мобильных вычислительных средствах вследствие ограниченной пропускной способности сети и (или) из-за того, что переносное оборудование не может быть подсоединено на время, которое запланировано для резервирования.

11.7.2 Дистанционная работа

Мера и средство контроля и управления

Политика, планы и процедуры эксплуатации должны быть разработаны и внедрены для дистанционной работы.

Рекомендация по реализации

Организации должны разрешать дистанционную работу только при уверенности в том, что применяются соответствующие соглашения о безопасности и меры и средства контроля и управления, которые, в свою очередь, согласуются с политикой безопасности организации.

Следует обеспечить необходимую защиту места дистанционной работы в отношении, например хищения оборудования и информации, несанкционированного раскрытия информации, несанкционированного удаленного доступа к внутренним системам организации или неправильного использования оборудования. Дистанционная работа должна быть санкционирована и контролируема руководством, и должна быть обеспечена уверенность в том, что имеются соответствующие меры для данного способа работы.

Необходимо принимать во внимание следующее:

a) существующую физическую безопасность места дистанционной работы, включая физическую безопасность здания и окружающей среды;

b) предлагаемые условия дистанционной работы;

c) требования в отношении безопасности коммуникаций, учитывая потребность в удаленном доступе к внутренним системам организации, чувствительность информации, к которой будет осуществляться доступ и которая будет передаваться по каналам связи, а также чувствительность самих внутренних систем;

d) угрозу несанкционированного доступа к информации или ресурсам со стороны других лиц, использующих место дистанционной работы, например членов семьи и друзей;

e) использование домашних компьютерных сетей, а также требования или ограничения в отношении конфигурации услуг беспроводных сетей;

f) политики и процедуры для предотвращения споров, касающихся прав на интеллектуальную собственность, разработанную на оборудовании, находящемся в частной собственности;

g) доступ к оборудованию, находящемуся в частной собственности (для проверки безопасности машины или во время проведения расследований), который может быть запрещен законодательством;

h) лицензионные соглашения в отношении программного обеспечения, которые таковы, что организация может стать ответственной за лицензирование клиентского программного обеспечения на рабочих станциях, находящихся в частной собственности сотрудников, подрядчиков или пользователей третьей стороны;

i) требования в отношении антивирусной защиты и межсетевых экранов.

Рекомендации и необходимые организационные меры включают, в частности:

a) обеспечение подходящим оборудованием и мебелью для дистанционной работы в тех случаях, когда запрещается использование оборудования, находящегося в частной собственности, если оно не находится под контролем организации;

b) определение видов разрешенной работы, времени работы, классификацию информации, которая может поддерживаться внутренними системами и услугами, к которым разрешен доступ сотруднику в дистанционном режиме;

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

d) физическую безопасность;

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

f) обеспечение технической поддержки и обслуживания аппаратного и программного обеспечения;

g) обеспечение страхования;

h) процедуры в отношении резервного копирования данных и обеспечения непрерывности бизнеса;

i) аудит и мониторинг безопасности;

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

Дополнительная информация

При работе в дистанционном режиме применяются коммуникационные технологии, дающие возможность сотрудникам работать в конкретном удаленном месте за пределами своей организации.

12 Приобретение, разработка и эксплуатация информационных систем

12.1 Требования безопасности информационных систем

Цель: Обеспечить уверенность в том, что безопасность является неотъемлемой частью информационных систем.

Информационные системы включают эксплуатируемые системы, инфраструктуру, прикладные программы бизнеса, готовые продукты, услуги и прикладные программы, разработанные пользователями. Проектирование и внедрение информационной системы, поддерживающей процесс бизнеса, может быть критичным с точки зрения безопасности. Требования безопасности следует выявлять и согласовывать до разработки и (или) внедрения информационных систем.

Все требования безопасности следует выявлять на стадии определения задач проекта, а также обосновывать, согласовывать и документально оформлять в рамках общего проекта по внедрению информационной системы.

12.1.1 Анализ требований безопасности и спецификация

Мера и средство контроля и управления

Необходимо, чтобы в формулировках требований бизнеса для новых информационных систем или при модернизации существующих информационных систем были определены требования к мерам и средствам контроля и управления безопасности.

Рекомендация по реализации

В спецификациях требований к мерам и средствам контроля и управления следует учитывать как встроенные в информационную систему автоматизированные меры и средства контроля и управления, так и необходимость поддержки ручного управления. Аналогично следует подходить к оценке пакетов прикладных программ, разработанных или приобретенных для прикладных программ бизнеса.

Необходимо, чтобы требования безопасности и соответствующие меры и средства контроля и управления отражали ценность информационных активов (см. 7.2) и потенциальный ущерб бизнесу, который мог бы явиться результатом недостаточности мер безопасности или их отсутствия.

Системные требования в отношении информационной безопасности и процессов реализации безопасности необходимо включать на ранних стадиях проектов, касающихся информационных систем. Определение мер и средств контроля и управления на стадии проектирования системы позволяет существенно снизить затраты на их внедрение и поддержку по сравнению с разработкой мер и средств контроля и управления во время или после внедрения системы.

В случае приобретения готовых продуктов необходимо соблюдение формального процесса приобретения и тестирования. В договорах с поставщиками должны учитываться определенные требования безопасности. Если функциональность безопасности в предлагаемом готовом продукте не удовлетворяет установленному организацией требованию, то тогда необходимо повторно рассмотреть порождаемый этим фактом риск и связанные с ним меры и средства контроля и управления прежде, чем продукт будет приобретен. Если обеспечивается дополнительная функциональность, и это создает риск безопасности, то ее следует блокировать, или пересмотреть предлагаемую структуру управления, чтобы определить возможность использования преимуществ имеющейся дополнительной функциональности.

Дополнительная информация

Если признано целесообразным, например из соображений затрат, руководство может пожелать воспользоваться независимой оценкой и сертификацией продуктов. Дополнительную информацию о критериях оценки безопасности продуктов ИТ можно найти в ИСО/МЭК 15408 или других стандартах по сертификации или оценке.

ИСО/МЭК ТО 13335-3 содержит рекомендации по использованию процессов менеджмента риска для определения требований к мерам и средствам контроля и управления безопасностью.

12.2 Корректная обработка в прикладных программах

Цель: Предотвратить ошибки, потерю, неавторизованную модификацию или нецелевое использование информации в прикладных программах.

Соответствующие меры и средства контроля и управления необходимо предусмотреть в прикладных программах, включая прикладные программы, разработанные пользователем, для обеспечения уверенности в корректности обработки данных. Указанные меры и средства контроля и управления должны также включать возможность подтверждения корректности ввода, обработки и вывода данных.

Дополнительные меры и средства контроля и управления могут потребоваться для систем, которые обрабатывают или оказывают воздействие на чувствительную, ценную или критическую информацию. Такие меры и средства контроля и управления безопасности должны быть определены на основе требований безопасности и оценки рисков.

12.2.1 Подтверждение корректности входных данных

Мера и средство контроля и управления

Входные данные для прикладных программ должны проходить процедуру подтверждения с целью обеспечения уверенности в их корректности и соответствии.

Рекомендация по реализации

Проверки следует проводить при вводе транзакций бизнеса, справочников (например имена и адреса, кредитные лимиты, идентификационные номера клиентов) и таблиц параметров (например цены продаж, курсы валют, ставки налогов). Необходимо рассмотреть следующие рекомендации:

а) двойной ввод или другие процедуры проверки ввода, например проверка границ или ограничение полей до определенных диапазонов вводимых данных с целью обнаружения следующих ошибок:

1) значений, выходящих за допустимый диапазон;

2) недопустимых символов в полях данных;

3) отсутствующих или неполных данных;

4) превышения верхних и нижних пределов объема данных;

5) запрещенных или противоречивых контрольных данных;

b) периодическая проверка содержимого ключевых полей или файлов данных для подтверждения их достоверности и целостности;

c) сверка печатных копий вводимых документов на предмет выявления любых несанкционированных изменений (необходимо, чтобы все изменения во вводимых документах были утверждены);

d) процедуры реагирования на ошибки проверки;

e) процедуры проверки достоверности вводимых данных;

f) определение обязанностей всех сотрудников, вовлеченных в процесс ввода данных;

g) создание журнала регистрации действий, связанных с процессом ввода данных (см. 10.10.1).

Дополнительная информация

Там, где это целесообразно, можно рассмотреть автоматическую экспертизу и проверку вводимых данных, чтобы снизить риск ошибок и предотвратить стандартные атаки, включая переполнение буфера и внесение кода.

12.2.2 Управление внутренней обработкой

Мера и средство контроля и управления

Подтверждающие проверки должны быть включены в прикладные программы с целью обнаружения любого искажения информации вследствие ошибок обработки или преднамеренных действий.

Рекомендация по реализации

Разработка и реализация прикладных программ должны обеспечивать уверенность в том, что риски обработки сбоев, ведущих к потере целостности, сведены к минимуму. Необходимо учитывать, в частности, следующее:

a) использование функций добавления, модификации и удаления для осуществления изменений данных;

b) процедуры, не допускающие запуск программ, исполняемых в неправильной последовательности или исполняемых после сбоя в предшествующей обработке (см. 10.1.1);

c) использование соответствующих программ для восстановления после сбоев и обеспечение правильной обработки данных;

d) защиту от атак, использующих перегрузки/переполнения буфера.

Необходимо подготавливать соответствующую технологическую карту, действия документально оформлять и надежно хранить результаты. Примеры проверок, которые могут быть комбинированными, включают следующее:

a) контроль сеансовой или пакетной обработки с целью согласования остатков массива данных после обновлений в результате транзакции;

b) контроль баланса, чтобы проверить соответствие открываемых данных и данных предыдущего закрытия, а именно:

1) меры и средства контроля и управления «от-выполнения-к-выполнению»;

2) суммарное количество обновлений файла;

3) контроль «от-программы-к-программе»;

c) подтверждение корректности данных, сгенерированных системой (см. 12.2.1);

d) проверки целостности, аутентичности или какого-либо другого свойства безопасности, полученных данных или программного обеспечения, или передаваемых 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 прикладные 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, связанных с обработкой (см. 10.10.1).

Дополнительная информация

Данные, которые были введены правильно, могут быть искажены вследствие аппаратных ошибок, ошибок обработки или преднамеренных действий. Обоснование необходимых проверок зависит от характера прикладной программы и влияния на бизнес любого искажения данных.

12.2.3 Целостность сообщений

Мера и средство контроля и управления

Необходимо определить требования в отношении обеспечения аутентичности и защиты целостности сообщений в прикладных программах, а также идентифицировать и внедрить соответствующие меры и средства контроля и управления.

Рекомендация по реализации

Следует проводить оценку рисков безопасности для определения необходимости обеспечения целостности сообщений, и идентификации соответствующего способа реализации.

Дополнительная информация

Криптографические методы (см. 12.3) могут использоваться как соответствующее средство реализации аутентификации сообщений.

12.2.4 Подтверждение выходных данных

Мера и средство контроля и управления

Данные, выводимые из прикладной программы, должны быть проверены с целью обеспечения уверенности в корректности обработки хранимой информации и соответствия требованиям.

Рекомендация по реализации

Проверка выходных данных может включать:

a) проверки достоверности с целью определения приемлемости выходных данных;

b) контрольная сверка результатов, для обеспечения уверенности в том, что все данные были обработаны;

c) предоставление достаточной информации для чтения или последующей системы обработки, чтобы определить корректность, полноту, точность и классификацию информации;

d) процедуры реагирования на проверку пригодности выходных данных;

e) определение обязанностей всех сотрудников, вовлеченных в процесс вывода данных;

f) создание журнала регистрации действий по подтверждению корректности выходных данных.

Дополнительная информация

Как правило, системы и прикладные программы построены на предпосылке, что при наличии соответствующих подтверждений корректности, проверок и тестирования, выводимые данные будут всегда правильны. Но это не всегда так, т. е. при некоторых обстоятельствах, протестированные системы будут по-прежнему производить некорректные данные вывода.

12.3 Криптографические меры и средства контроля и управления

Цель: Защищать конфиденциальность, аутентичность или целостность информации, используя криптографические средства.

Необходимо разработать политику в отношении использования криптографических мер и средств контроля и управления. Для поддержки использования криптографических методов следует применять управление ключами.

12.3.1 Политика использования криптографических мер и средств контроля и управления

Мера и средство контроля и управления

В целях защиты информации необходимо разработать и реализовать политику в отношении использования криптографических мер и средств контроля и управления.

Рекомендация по реализации

При разработке криптографической политики необходимо учитывать следующее:

a) позицию руководства в отношении использования средств криптографии во всей организации, включая общие принципы, в соответствии с которыми должна быть защищена бизнес-информация (см. 5.1.1);

b) основанный на оценке риска требуемый уровень защиты, который должен быть определен с учетом типа, стойкости и качества требуемого алгоритма шифрования;

c) использование шифрования для защиты чувствительной информации, передаваемой с помощью переносных или сменных носителей и устройств или по линиям связи;

d) подход к управлению ключами, включая методы по защите криптографических ключей и восстановлению зашифрованной информации в случае потери, компрометации или повреждения ключей;

e) роли и обязанности, например персональная ответственность за:

1) внедрение политики;

2) управление ключами, включая генерацию ключей (см. 12.3.2);

f) стандарты, которые должны быть приняты для эффективной реализации во всей организации (какое решение используется и для каких процессов бизнеса);

g) влияние использования зашифрованной информации на меры и средства контроля и управления, которые базируются на проверки содержимого (например обнаружение вирусов).

При внедрении политики организации в области криптографии следует учитывать требования законодательства и ограничения, которые могут применяться в отношении криптографических методов в различных странах, а также вопросы трансграничного потока зашифрованной информации (см. 15.1.6).

Криптографические меры и средства контроля и управления могут использоваться для достижения различных целей безопасности, например:

a) конфиденциальности посредством использования шифрования информации для защиты чувствительной или критической информации как хранимой, так и передаваемой;

b) целостности/аутентичности посредством использования цифровых подписей или кодов аутентификации сообщений для защиты аутентичности и целостности, хранимой или передаваемой чувствительной или критической информации;

c) неотказуемости, посредством использования криптографических методов для получения подтверждения того, что событие или действие имело или не имело место.

Дополнительная информация

Процесс принятия решения относительно использования криптографии следует рассматривать в рамках более общего процесса оценки рисков и выбора мер и средств контроля и управления. Такая оценка может затем использоваться для определения того, является ли криптографическая мера и средство контроля и управления подходящей, какой тип мер и средств контроля и управления следует применять, с какой целью и для каких процессов бизнеса.

Политика использования криптографических мер и средств контроля и управления необходима для того, чтобы максимизировать выгоду и минимизировать риски использования криптографических методов, и чтобы избежать неадекватного или неправильного использования данных средств. При использовании цифровых подписей, необходимо учитывать все применимые требования законодательства, в особенности законодательных актов, описывающих условия, при которых цифровая подпись имеет юридическую силу (см. 15.1).

Следует проконсультироваться со специалистами для определения необходимого уровня защиты, выбора подходящих технических требований, которые обеспечат требуемую защиту и поддержку реализации безопасной системы управления ключами (см. 12.3.2).

ПК 27 СТК 1 ИСО/МЭК разработал несколько стандартов по мерам и средствам контроля и управления, связанным с использованием криптографии. Более подробную информацию можно найти также в [17] и [18].

12.3.2 Управление ключами

Мера и средство контроля и управления

Для поддержки использования организацией криптографических методов необходимо применять управление ключами.

Рекомендация по реализации

Все криптографические ключи следует защищать от модификации, потери и разрушения. Кроме того, секретным и персональным ключам необходима защита от несанкционированного раскрытия. Оборудование, используемое для генерации, хранения и архивирования ключей должно быть физически защищено.

Система управления ключами должна быть основана на согласованном множестве стандартов, процедур и безопасных методов для:

a) генерации ключей для различных криптографических систем и прикладных программ;

b) генерации и получения сертификатов открытых ключей;

c) рассылки ключей предполагаемым пользователям, включая инструкции по активации указанных ключей при получении;

d) хранения ключей, в том числе инструкций в отношении получения доступа к ключам авторизованных пользователей;

e) замены или обновления ключей, включая правила в отношении порядка и сроков замены ключей;

f) действий в отношении скомпрометированных ключей;

g) аннулирования ключей, в том числе порядок изъятия и деактивации, например в случае компрометации ключей или при увольнении пользователя из организации (при этом ключи необходимо также архивировать);

h) восстановления ключей, которые были утеряны или испорчены, как часть менеджмента непрерывности бизнеса, например для восстановления зашифрованной информации;

i) архивирования ключей, например для восстановления заархивированной или резервной информации;

j) уничтожения информации;

k) регистрации и аудита действий, связанных с управлением ключами.

Для уменьшения вероятности компрометации ключей необходимо, чтобы они имели определенные даты активации и деактивации. Данный период времени зависит от обстоятельств, при которых используются криптографические меры и средства контроля и управления, и от осознаваемого риска.

В дополнение к вопросу безопасности менеджмента секретных и персональных ключей, необходимо также учитывать вопросы аутентичности открытых ключей. Процесс аутентификации может осуществляться при использовании сертификатов открытых ключей, которые обычно выдаются органом сертификации, представляющим собой официально признанную организацию, применяющую соответствующие меры и средства контроля и управления и процедуры для обеспечения требуемой степени доверия.

Необходимо, чтобы соглашение об уровне обслуживания или договоры с внешними поставщиками услуг, связанных с криптографией, например с органом — держателем справочников сертификатов, включали положения относительно ответственности, надежности услуг и времени реагирования на запросы по их предоставлению (см. 6.2.3).

Дополнительная информация

Управление криптографическими ключами является существенным аспектом для эффективного использования криптографических средств. В ИСО/МЭК 11770 [6] содержится дополнительная информация об управлении ключами. Различаются два типа криптографических методов:

a) методы, применяемые в отношении секретных ключей, когда две или более стороны совместно используют один и тот же ключ, и этот ключ применяется как для шифрования, так и для дешифрования информации; данный 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 этот ключ;

b) методы, применяемые в отношении открытых ключей, где каждый пользователь имеет пару ключей, открытый ключ (который может быть показан любому) и секретный ключ (который должен храниться в секрете); методы с открытыми ключами могут использоваться для проверки и формирования цифровых подписей (см. также ИСО/МЭК 9796-2 [7], ИСО/МЭК 9796-3 [8] и ИСО/МЭК 14888-1 [9]).

Существует угроза подделки цифровой подписи и замены открытого ключа пользователя на фальсифицированный. Данная проблема решается с помощью органов — держателей сертификатов открытых ключей.

Криптографические методы могут также использоваться и для защиты криптографических ключей. Может потребоваться наличие процедур для обработки запросов правоохранительных органов на получение криптографических ключей, например для представления зашифрованной информации в незашифрованном виде в качестве доказательства в суде.

12.4 Безопасность системных файлов

Цель: Обеспечить уверенность в безопасности системных файлов.

Доступ к системным файлам и исходным текстам программ следует контролировать, а проекты ИТ и деятельности по их поддержке необходимо осуществлять безопасным способом. Необходимо проявлять осторожность в среде тестирования, чтобы не подвергать риску чувствительную информацию.

12.4.1 Управление эксплуатируемым программным обеспечением

Мера и средство контроля и управления

Необходимо применять процедуры контроля установки программного обеспечения в эксплуатируемых системах.

Рекомендация по реализации

Для сведения к минимуму риска повреждения эксплуатируемых систем необходимо учесть следующие рекомендации в отношении контроля изменений:

a) обновление эксплуатируемого программного обеспечения, прикладных программ и библиотек программ должны выполнять только обученные администраторы при наличии соответствующего разрешения руководства (см. 12.4.3);

b) эксплуатируемые системы должны содержать только утвержденный исполняемый программный код и не должны содержать коды разработки или компиляторы;

c) прикладные программы и программное обеспечение следует внедрять в эксплуатируемую систему только после всестороннего и успешного тестирования, которое должно выполняться на изолированных системах и включать в себя тесты на пригодность к эксплуатации, безопасность, влияние на другие системы и удобство для пользователя (см. 10.1.4); необходимо обеспечить уверенность в том, что все соответствующие библиотеки исходных текстов программ были обновлены;

d) меры и средства контроля и управления конфигурацией системы необходимо использовать согласно системной документации для сохранения управления всем реализуемым программным обеспечением;

e) прежде чем изменения будут реализованы, необходимо применять метод отката;

f) в контрольном журнале должны быть сохранены все обновления эксплуатируемой библиотеки программ;

g) предыдущие версии прикладного программного обеспечения следует сохранять на случай непредвиденных обстоятельств;

h) старые версии программного обеспечения следует архивировать вместе со всей требуемой информацией и параметрами, процедурами, конфигурационными деталями и поддерживающим программным обеспечением до тех пор, пока данные хранятся в архиве.

Необходимо, чтобы поставляемое поставщиком программное обеспечение, используемое в действующей системе, поддерживалось на уровне, обеспечиваемом поставщиком. Со временем поставщики программного обеспечения прекращают поддерживать более старые версии программного обеспечения. Организация должна учитывать риски, когда она полагается на неподдерживаемое программное обеспечение.

Любое решение об обновлении программного обеспечения до новой версии должно учитывать требования бизнеса в отношении изменения и безопасности новой версии, т. е., введение новых функциональных возможностей безопасности или количество и серьезность проблем безопасности, связанных с этой версией. Исправления (патчи) программного обеспечения следует применять, если они помогают удалять или снижать уязвимости безопасности (см. 12.6.1).

Физический или логический доступ следует предоставлять поставщикам только для целей поддержки, по мере необходимости и на основании разрешения руководства. Действия поставщика должны подвергаться мониторингу.

Программное обеспечение компьютеров может использовать поставляемые внешним (иностранным) поставщиком программное обеспечение и модули, которые должны быть контролируемы и управляемы во избежание несанкционированных изменений, которые могут способствовать нарушению безопасности.

Дополнительная информация

Эксплуатируемую систему следует обновлять только при необходимости, например, если текущая версия эксплуатируемой системы больше не удовлетворяет требованиям бизнеса. Обновление не следует проводить только потому, что доступна новая версия для эксплуатируемой системы. Новые версии систем, находящихся в промышленной эксплуатации, могут быть менее безопасными, менее стойкими и менее понятными, чем текущие системы.

12.4.2 Защита тестовых данных системы

Мера и средство контроля и управления

Данные тестирования следует тщательно отбирать, защищать и контролировать.

Рекомендация по реализации

Следует избегать использования действующих баз данных, содержащих персональную или какую-либо другую чувствительную информацию, для целей тестирования. Если персональная или какая-либо другая чувствительная информация требуется для тестирования, то все чувствительные подробности и информационное наполнение следует удалить или изменить до неузнаваемости перед использованием. Для защиты действующих (рабочих) данных, если они используются для целей тестирования, необходимо применять следующие рекомендации:

a) процедуры управления доступом, применимые для эксплуатируемых прикладных систем, следует также применять и для тестирования прикладных систем;

b) необходимо отдельное разрешение на каждый случай копирования действующей (рабочей) информации для тестирования прикладной системы;

c) после того как тестирование было завершено, действующую (рабочую) информацию следует немедленно удалить из тестируемой прикладной системы;

d) копирование и использование действующей (рабочей) информации должно фиксироваться для обеспечения контрольной записи.

Дополнительная информация

Для осуществления системного или приемочного тестирования обычно требуется существенный объем тестовых данных, которые максимально приближены к действующим (рабочим) данным.

12.4.3 Управление доступом к исходным текстам программ

Мера и средство контроля и управления

Доступ к исходным текстам программ необходимо ограничивать.

Рекомендация по реализации

В целях предотвращения введения несанкционированных функциональных возможностей и во избежание непреднамеренных изменений должен быть обеспечен строгий контроль доступа к исходным текстам программ и связанным с ними документам (например проектам, спецификациям, планам верификации и планам валидации). В отношении исходных текстов программ это может быть достигнуто с помощью контролируемого централизованного хранения таких текстов, предпочтительнее в библиотеках исходных текстов программ. Чтобы сократить возможность искажения компьютерных программ, необходимо рассмотреть следующие рекомендации (см. 11) по управлению доступом к таким библиотекам исходных текстов программ:

a) по возможности, следует избегать хранения библиотек исходных текстов программ в эксплуатируемых системах;

b) менеджмент исходных текстов программ и библиотек исходных текстов программ следует осуществлять в соответствии с установленными процедурами;

c) персонал поддержки не должен иметь неограниченный доступ к библиотекам исходных текстов программ;

d) обновление библиотек исходных текстов программ и связанных с ними элементов, а также предоставление программистам исходных текстов программ должны осуществляться только после получения соответствующего разрешения;

e) распечатки (листинги) программ следует хранить безопасным образом (см. 10.7.4);

f) в контрольном журнале должны фиксироваться все обращения к библиотекам исходных текстов программ;

g) поддержку и копирование библиотек исходных текстов программ следует осуществлять в соответствии со строгими процедурами контроля изменений (см. 12.5.1).

Дополнительная информация

Исходный текст программы — это текст, написанный программистами, который компилируется (и компонуется) с целью создания исполняемых файлов. Определенные языки программирования формально не проводят различия между исходным текстом программ и исполняемыми файлами, поскольку исполняемые файлы создаются в то время, когда они активированы.

В стандартах ИСО 10007 [13] и ИСО/МЭК 12207 [14] содержится дополнительная информация об управлении конфигурацией и о процессе, связанном с жизненным циклом программного обеспечения.

12.5 Безопасность в процессах разработки и поддержки

Цель: Поддерживать безопасность прикладных систем и информации.

Необходимо строго контролировать среды проектирования и поддержки.

Необходимо, чтобы руководители, ответственные за прикладные системы, также несли ответственность и за безопасность среды проектирования или поддержки. Они должны обеспечить уверенность в том, что все предложенные изменения системы проанализированы на предмет возможных нарушений безопасности системы или условий эксплуатации.

12.5.1 Процедуры управления изменениями

Мера и средство контроля и управления

Внесение изменений следует контролировать, используя формальные процедуры управления изменениями.

Рекомендация по реализации

Для сведения к минимуму повреждений информационных систем следует осуществлять и документально оформлять формальные процедуры контроля изменений. Введение новых и значительные изменения существующих систем должны сопровождаться формальным процессом документального оформления, детализирования, тестирования, контроля качества и управляемого внедрения.

Указанный процесс должен включать в себя оценку рисков, анализ влияния изменений и детализацию необходимых мер и средств контроля и управления безопасности. Он также должен обеспечивать

уверенность в том, что не нарушены безопасность и сами процедуры управления, что программистам, отвечающим за поддержку, предоставлен доступ только к тем частям системы, которые необходимы для их работы, и что любые изменения формально согласованы и одобрены.

По возможности, прикладные программы и эксплуатационные процедуры управления изменениями должны быть интегрированы (см. 10.1.2). Процедуры изменения должны включить:

a) ведение учета согласованных уровней разрешений;

b) обеспечение уверенности в том, что изменения представлены уполномоченными пользователями;

c) анализ мер и средств контроля и управления, а также процедур целостности на предмет обеспечения уверенности в том, что они не будут нарушены изменениями;

d) выявление всего программного обеспечения, информации, объектов баз данных и аппаратных средств, требующих изменений;

e) получение формального одобрения на детальные предложения по изменениям перед началом работы;

f) обеспечение уверенности в том, что авторизованный пользователь одобрил все изменения до их реализации;

g) обеспечение уверенности в том, что комплект системной документации обновляется после завершения каждого изменения, и что старая документация архивируется или удаляется;

h) поддержание управления версиями для всех обновлений программного обеспечения;

i) сохранение контрольных записей обо всех запросах на изменение;

j) обеспечение уверенности в том, что эксплуатационная документация (см. 10.1.1) и пользовательские процедуры при необходимости изменяются, чтобы соответствовать внесенным изменениям;

k) обеспечение уверенности в том, что процесс внедрения изменений осуществляется в согласованное время и не нарушает затрагиваемых процессов бизнеса.

Дополнительная информация

Изменение в программном обеспечении может повлиять на среду эксплуатации.

Общепринятая практика включает в себя тестирование нового программного обеспечения в среде, которая отделена от среды эксплуатации и среды разработки (см. также 10.1.4). Это обеспечивает средства контроля над новым программным обеспечением, и предоставляет дополнительную защиту действующей (рабочей) информации, используемой в целях тестирования. Для этих целей следует использовать изменения (патчи), служебные пакеты обновлений и другие обновления. Автоматические обновления не следует применять в критических системах, поскольку некоторые обновления могут являться причиной отказа критических прикладных программ (см. 12.6).

12.5.2 Техническая проверка прикладных программ после изменений эксплуатируемой системы

Мера и средство контроля и управления

При внесении изменений в эксплуатируемые системы прикладные программы, имеющие большое значение для бизнеса, следует анализировать и тестировать с целью обеспечения уверенности в том, что не оказывается неблагоприятного воздействия на функционирование или безопасность организации.

Рекомендация по реализации

Этот процесс должен охватывать:

a) анализ мер и средств контроля и управления прикладными программами и процедур целостности на предмет обеспечения уверенности в том, что они не будут нарушены изменениями эксплуатируемой системы;

b) обеспечение уверенности в том, что ежегодный план поддержки и бюджет предусматривает анализ и тестирование систем, необходимые при изменениях эксплуатируемой системы;

c) обеспечение уверенности в том, что уведомления об изменениях эксплуатируемой системы поступают своевременно, чтобы дать возможность перед их реализацией провести соответствующие тесты и анализы;

d) обеспечение уверенности в том, что соответствующие изменения вносятся в планы обеспечения непрерывности бизнеса (см. 14).

Определенной группе лиц или отдельному специалисту следует вменять в обязанность проведение мониторинга уязвимостей, версий патчей поставщиков и их установок (см. 12.6).

12.5.3 Ограничения на изменения пакетов программ

Мера и средство контроля и управления

Необходимо избегать модификаций пакетов программ, ограничиваться необходимыми изменениями и строго контролировать все сделанные изменения.

Рекомендация по реализации

Насколько возможно и допустимо с практической точки зрения пакеты программ, поставляемые поставщиком, следует использовать без изменений. Там, где необходимо внести изменения в пакет программ, следует учитывать следующее:

a) риск в отношении встроенных мер и средств контроля и управления и процедур обеспечения целостности;

b) необходимость получения согласия поставщика;

c) возможность получения требуемых изменений от поставщика в качестве стандартной программы обновления;

d) возможные последствия в случае, если организация станет ответственной за будущее сопровождение программного обеспечения в результате внесенных изменений.

Если необходимо внесение изменений, то оригинальное программное обеспечение следует сохранить, а изменения вносить в четко определенную копию. Следует реализовывать процесс управления обновлением программного обеспечения, чтобы иметь уверенность в том, что для всего разрешенного программного обеспечения устанавливаются новейшие одобренные к применению патчи и обновления прикладных программ (см. 12.6). Все изменения необходимо полностью тестировать и документально оформлять таким образом, чтобы их можно было использовать повторно для будущих обновлений программного обеспечения. При необходимости изменения должны быть проверены и подтверждены независимой оценочной организацией.

12.5.4 Утечка информации

Мера и средство контроля и управления

Возможность утечки информации должна быть предотвращена.

Рекомендация по реализации

Для снижения риска утечки информации, например по причине использования и эксплуатации скрытых каналов, необходимо принимать во внимание следующее:

a) сканирование носителей исходящей информации и каналов связи на наличие скрытой информации;

b) маскирование и регулирование поведения систем и каналов связи для снижения вероятности того, что третья сторона сможет извлечь информацию из поведения систем и каналов связи;

c) использование систем и программного обеспечения, которые считаются максимально достоверными, например использование оцененных продуктов (см. ИСО/МЭК 15408);

d) регулярный мониторинг деятельности персонала и систем там, где это разрешено существующим законодательством или предписаниями;

e) мониторинг использования ресурсов в компьютерных системах.

Дополнительная информация

Скрытые каналы — это каналы, не предназначенные для передачи информационных потоков, но которые, тем не менее, могут существовать в системе или сети. Например манипулирование битами в пакетах протоколов связи может использоваться как скрытый метод передачи сигналов. Природа скрытых каналов такова, что предотвратить существование всех возможных скрытых каналов затруднительно или даже невозможно. Однако такие каналы часто используются «троянскими» программами (см. 10.4.1). Следовательно, принятие мер по защите от «троянских» программ снижает риск использования скрытых каналов.

Предотвращение неавторизованного доступа к сети (см. 11.4), а также политики и процедуры, препятствующие неправильному использованию информационных услуг персоналом (см. 15.1.5), способствуют защите от скрытых каналов.

12.5.5 Аутсорсинг разработки программного обеспечения

Мера и средство контроля и управления

Аутсорсинг разработки программного обеспечения должен быть под наблюдением и контролем организации.

Рекомендация по реализации

Там, где для разработки программного обеспечения привлекается сторонняя организация, необходимо учитывать следующее:

a) лицензионные соглашения, права собственности на программы и права интеллектуальной собственности (см. 15.1.2);

b) сертификацию качества и точности выполненной работы;

c) соглашения условного депонирования на случай отказа сторонней организации выполнять свои обязательства;

d) права доступа с целью проверки качества и точности сделанной работы;

e) договорные требования к качеству и функциональной безопасности программ;

f) тестирование программ перед установкой на предмет обнаружения вредоносных и «троянских» программ.

12.6 Менеджмент технических уязвимостей

Цель: Снизить риски, являющиеся результатом использования опубликованных технических уязвимостей.

Менеджмент технических уязвимостей следует осуществлять эффективным, систематическим и повторяемым способом, с проведением измерений с целью подтверждения его эффективности. Эти соображения должны касаться эксплуатируемых систем и любых других используемых прикладных программ.

12.6.1 Управление техническими уязвимостями

Мера и средство контроля и управления

Необходимо получать своевременную информацию о технических уязвимостях используемых информационных систем, оценивать незащищенность организации в отношении таких уязвимостей и принимать соответствующие меры для рассмотрения связанного с ними риска.

Рекомендация по реализации

Постоянно обновляемая и полная опись активов (см. 7.1) является предпосылкой эффективного менеджмента технических уязвимостей. Специальная информация, необходимая для поддержки менеджмента технических уязвимостей, включает в себя информацию о поставщике программного обеспечения, номерах версий, текущем состоянии развертывания (например какое программное обеспечение установлено на каких системах) и специалисте(ах), отвечающем(их) в организации за программное обеспечение.

Аналогично, своевременное действие должно предприниматься в ответ на выявление потенциальных технических уязвимостей. Для создания эффективного процесса менеджмента в отношении технических уязвимостей необходимо выполнять следующие рекомендации:

a) в организации необходимо определять и устанавливать роли и обязанности, связанные с менеджментом технических уязвимостей, включая мониторинг уязвимостей, оценку риска проявления уязвимостей, исправление программ (патчинг), слежение за активами и любые другие координирующие функции;

b) информационные ресурсы, которые будут использоваться для выявления значимых технических уязвимостей и обеспечения осведомленности о них, следует определять для программного обеспечения и другой технологии на основе списка инвентаризации активов (см. 7.1.1); эти информационные ресурсы должны обновляться вслед за изменениями, вносимыми в опись, или когда найдены другие новые или полезные ресурсы;

c) необходимо определить временные параметры реагирования на уведомления о потенциально значимых технических уязвимостях;

d) после выявления потенциальной технической уязвимости организация должна определить связанные с ней риски и действия, которые необходимо предпринять; такие действия могут включать внесение исправлений в уязвимые системы и (или) применение других мер и средств контроля и управления;

e) в зависимости от того, насколько срочно необходимо рассмотреть техническую уязвимость, предпринимаемое действие следует осуществлять в соответствии с мерами и средствами контроля и управления, связанными с менеджментом изменений (см. 12.5.1), или следуя процедурам реагирования на инциденты информационной безопасности (см. 13.2);

f) если имеется возможность установки патча, следует оценить риски, связанные с его установкой (риски, создаваемые уязвимостью, необходимо сравнить с риском установки патча);

g) перед установкой патчи следует тестировать и оценивать для обеспечения уверенности в том, что они являются эффективными и не приводят к побочным эффектам, которые нельзя допускать; если нет возможности установить патч, следует рассмотреть другие меры и средства контроля и управления, например:

1) отключение сервисов, связанных с уязвимостью;

2) адаптацию или добавление средств управления доступом, например межсетевых экранов на сетевых границах (см. 11.4.5);

3) усиленный мониторинг для обнаружения или предотвращения реальных атак;

4) повышение осведомленности об уязвимостях;

h) в контрольный журнал следует вносить информацию о всех предпринятых процедурах;

i) следует регулярно проводить мониторинг и оценку процесса менеджмента технических уязвимостей в целях обеспечения уверенности в его эффективности и действенности;

j) в первую очередь следует обращать внимание на системы с высоким уровнем риска.

Дополнительная информация

Правильное функционирование процесса менеджмента технических уязвимостей играет важную роль для многих организаций, поэтому процесс должен подвергаться регулярному мониторингу. Для обеспечения уверенности в том, что потенциально значимые технические уязвимости выявлены, важна точная инвентаризация.

Менеджмент технических уязвимостей может рассматриваться как подфункция менеджмента изменений и в качестве таковой может воспользоваться процессами и процедурами менеджмента изменений (см. 10.1.2 и 12.5.1).

Поставщики часто испытывают на себе значительное давление, заключающееся в требовании выпускать патчи в кратчайшие сроки. Поэтому патч не может решить проблему адекватно и может иметь побочные эффекты. К тому же, в некоторых случаях, если патч был однажды применен, деинсталлировать его может быть нелегко.

Если адекватное тестирование патчей провести не удается, например по причине затрат или отсутствия ресурсов, можно рассмотреть задержку в осуществлении внесения изменений, чтобы оценить связанные с этим риски, основанные на опыте других пользователей.

13 Менеджмент инцидентов информационной безопасности

13.1 Оповещение о событиях и уязвимостях информационной безопасности

Цель: Обеспечить уверенность в том, что о событиях и уязвимостях информационной безопасности оповещается способом, который позволяет своевременно предпринять корректирующее действие.

Необходимо использовать формальные процедуры информирования и эскалации[1)]. Все сотрудники, подрядчики и представители третьей стороны должны быть осведомлены о процедурах информирования, о различных типах событий и уязвимостях, которые могли бы оказать негативное влияние на безопасность активов организации. Они должны незамедлительно сообщать о любых событиях и уязвимостях информационной безопасности определенному контактному лицу.

13.1.1 Оповещение о событиях информационной безопасности

Мера и средство контроля и управления

О событиях информационной безопасности необходимо незамедлительно сообщать через соответствующие каналы управления.

Рекомендация по реализации

Необходимо внедрить формальную процедуру оповещения о событиях информационной безопасности вместе с процедурой реагирования и эскалации инцидента, содержащую действие, которое нужно предпринять при получении сообщения о событии информационной безопасности. Должна быть установлена «точка контакта» для уведомления о событиях информационной безопасности. Необходимо обеспечить уверенность в том, что эта «точка контакта» известна в организации, всегда доступна и способна к адекватному и своевременному реагированию.

Все сотрудники, подрядчики и представители третьей стороны должны быть осведомлены о своей обязанности незамедлительно сообщать о любых событиях информационной безопасности. Они должны быть также осведомлены о процедуре информирования о событиях информационной безопасности и «точке контакта». Необходимо, чтобы процедуры информирования включали:

a) соответствующие процессы обратной связи, для обеспечения уверенности в том, что сотрудник, сообщивший о событиях информационной безопасности, был уведомлен о результатах после того, как проблема была решена и закрыта;

[1)] В контексте менеджмента инцидентов информационной безопасности под термином «процедуры эскалации» понимается передача расследования инцидента на более высокий уровень в случае невозможности проведения адекватного расследования на более низком уровне.

b) формы сообщений о событиях информационной безопасности, которые должны напомнить лицу о действиях, которые необходимо совершить;

c) правила поведения в случае, если произойдет событие информационной безопасности, а именно:

1) сразу же обращать внимание на все важные детали (например тип несоответствия или недостатка, возникшие неисправности, сообщения на экране, странное поведение);

2) не предпринимать самостоятельно никакого действия, а немедленно сообщить в «точку контакта»;

d) ссылку на установленные формальные дисциплинарные процессы относительно сотрудников, подрядчиков и пользователей третьей стороны, которые нарушают правила безопасности.

Среда с высоким уровнем риска может быть оснащена сигнализацией о принуждении[1)], с помощью которой лица, на которые оказывается давление, могут указать на такие проблемы. Процедура реагирования на сигнализацию о принуждении должна отражать место высокого риска, которое показывает сигнализация.

Дополнительная информация

Примерами событий и инцидентов информационной безопасности могут быть:

a) потеря услуг, оборудования или средств обслуживания;

b) неисправности в системе или перегрузки;

c) ошибки оператора;

d) несоблюдение политик или рекомендаций;

e) нарушения мер физической безопасности;

f) неконтролируемые изменения систем;

g) программный или аппаратный сбой;

h) нарушения доступа.

Обращая должное внимание на аспекты конфиденциальности, можно для повышения осведомленности пользователей использовать инциденты информационной безопасности (см. 8.2.2) в качестве примеров того, что могло бы произойти, как реагировать на такие инциденты и как избежать их в будущем. Чтобы иметь возможность должным образом рассмотреть события и инциденты информационной безопасности, необходимо собирать свидетельства как можно быстрее после происшествия (см. 13.2.3).

Неисправная работа или другое аномальное поведение системы может служить показателем атаки на безопасность или реального недостатка безопасности, поэтому о них следует сообщать как о событии информационной безопасности.

Дополнительную информацию относительно отчетности о событиях информационной безопасности и о менеджменте инцидентов информационной безопасности можно найти в ИСО/МЭК ТО 18044 [20].

13.1.2 Оповещение об уязвимостях безопасности

Мера и средство контроля и управления

От всех сотрудников, подрядчиков и представителей третьей стороны, имеющих дело с информационными системами и услугами, необходимо требовать, чтобы они обращали внимание и сообщали о любых замеченных или предполагаемых уязвимостях в области безопасности в отношении систем или услуг.

Рекомендация по реализации

Все сотрудники, подрядчики и представители третьей стороны должны как можно быстрее сообщать об уязвимостях безопасности своему руководству или непосредственно поставщику услуг, чтобы предотвратить инциденты информационной безопасности. Механизм сообщения должен быть, насколько возможно, простым и доступным. Сотрудников, подрядчиков и представителей третьей стороны необходимо проинформировать о недопустимости попыток проверить предполагаемый недостаток.

Дополнительная информация

Сотрудникам, подрядчикам и представителям третьей стороны рекомендуется не проверять предполагаемые недостатки безопасности. Тестирование слабых мест защиты может быть интерпретировано как неправомочное использование системы, а также может нанести ущерб информационной системе или услуге и привести к юридической ответственности лица, выполнившего тестирование.

[1)] Сигнализация о принуждении — это способ, с помощью которого можно незаметно показать, что действие совершается «под принуждением».

13.2 Менеджмент инцидентов информационной безопасности и необходимое совершенствование

Цель: Обеспечить уверенность в том, что в отношении менеджмента инцидентов информационной безопасности применяется последовательный и эффективный подход.

Обязанности и процедуры должны осуществляться эффективным способом в отношении обработки событий и уязвимостей информационной безопасности, как только они были зарегистрированы. Процесс постоянного совершенствования необходимо применять в отношении мониторинга, оценки, общего менеджмента и реагирования на инциденты информационной безопасности.

Необходимо собирать доказательства, чтобы обеспечить уверенность в соответствии законодательным требованиям.

13.2.1 Обязанности и процедуры

Мера и средство контроля и управления

Необходимо устанавливать обязанности должностных лиц по осуществлению менеджмента и процедуры для обеспечения быстрого, эффективного и должного реагирования на инциденты информационной безопасности.

Рекомендация по реализации

В дополнение к информированию о событиях и недостатках информационной безопасности (см. 13.1), необходимо также использовать мониторинг систем, сигналов тревоги и уязвимостей для обнаружения инцидентов информационной безопасности (см. 10.10.2). В отношении процедур менеджмента инцидентов информационной безопасности необходимо учитывать следующие рекомендации:

a) следует установить процедуры обработки различных типов инцидентов информационной безопасности, включая:

1) сбои информационных систем и потерю обслуживания;

2) вредоносные программы (см. 10.4.1);

3) отказ в обслуживании;

4) ошибки, являющиеся следствием неполноты или неточности данных бизнеса;

5) нарушения конфиденциальности и целостности;

6) неправильное использование информационных систем;

b) в дополнение к обычным планам обеспечения непрерывности бизнеса (см. 14.1.3), процедуры должны также охватывать (см. 13.2.2):

1) анализ и выявление причины инцидента;

2) ограничение распространения последствий;

3) планирование и реализацию корректирующего действия для предотвращения повторения, если это необходимо;

4) взаимодействие с лицами, испытавшими влияние инцидента или участвовавшими в восстановлении после инцидента;

5) сообщение о предпринятом действии в соответствующий орган;

c) контрольные записи и аналогичные доказательства необходимо собирать (см. 13.2.3) и защищать для:

1) анализа внутренних проблем;

2) использования в качестве судебного доказательства в отношении возможного нарушения договора или нормативного требования, а также в случае гражданского или уголовного производства, например на основании неправильного использования компьютера или законодательства о защите данных;

3) обсуждения условий о выплате компенсации поставщиками программного обеспечения и услуг;

d) действия по восстановлению после проявления недостатков безопасности и по устранению сбоев систем следует тщательно контролировать; процедуры должны обеспечивать уверенность в том, что:

1) только четко идентифицированному и уполномоченному персоналу разрешен доступ к эксплуатируемым системам и данным (см. 6.2 на предмет внешнего доступа);

2) все предпринятые аварийные действия документируются в деталях;

3) руководство информируется об аварийном действии, и такое действие анализируется должным образом;

4) целостность систем, а также мер и средств контроля и управления бизнеса подтверждается с минимальной задержкой.

Цели менеджмента инцидентов информационной безопасности следует согласовать с руководством, а также необходимо обеспечить уверенность в том, что лица, ответственные за осуществление менеджмента инцидентов информационной безопасности, понимают приоритеты организации по обработке таких инцидентов.

Дополнительная информация

Инциденты информационной безопасности могут выходить за границы организаций и стран. В отношении реагирования на такие инциденты имеется растущая потребность в координации реагирования и в совместном использовании информации об этих инцидентах с внешними организациями, при необходимости.

13.2.2 Извлечение уроков из инцидентов информационной безопасности

Мера и средство контроля и управления

Должны быть созданы механизмы, позволяющие установить типы, объемы и убытки, вызванные инцидентами информационной безопасности, которые должны быть измерены и проконтролированы.

Рекомендация по реализации

Информацию, полученную в результате оценки инцидентов информационной безопасности, следует использовать для идентификации повторяющихся или оказывающих значительное влияние инцидентов.

Дополнительная информация

Оценка инцидентов информационной безопасности может указывать на необходимость совершенствования существующих мер или внедрения дополнительных мер и средств контроля и управления, чтобы снизить частоту, ущерб и стоимость возможных происшествий, или должна быть принята во внимание при пересмотре политики безопасности (см. 5.1.2).

13.2.3 Сбор доказательств

Мера и средство контроля и управления

В тех случаях, когда последующие действия против лица или организации после инцидента безопасности приводят к судебному иску (как гражданскому, так и уголовному), доказательства должны быть собраны, сохранены и представлены в соответствии с правилами сбора доказательств, изложенными в соответствующих юрисдикциях.

Рекомендация по реализации

При сборе и представлении доказательства для целей дисциплинарных воздействий, рассматриваемых в рамках организации, необходимо разработать и обеспечить следование внутренним процедурам.

В основном, правила, применяемые в отношении сбора доказательств, предусматривают:

a) допустимость доказательств, т. е. может ли доказательство использоваться в суде;

b) весомость доказательств, т. е. качество и полнота доказательств.

Чтобы добиться признания допустимости доказательств, организациям необходимо быть уверенными в том, что их информационные системы соответствуют любому изданному стандарту или своду правил в отношении предъявления допустимых доказательств.

Весомость предъявляемых доказательств должна соответствовать любым применимым требованиям. Чтобы добиться признания весомости доказательств, необходимы убедительные подтверждения того, что для корректной и последовательной защиты доказательств в течение периода их хранения и обработки применялись меры и средства контроля и управления соответствующего качества и полноты (т. е. доказательство управляемости процесса). В общем случае такие убедительные подтверждения могут быть получены следующим образом:

a) для бумажных документов: оригинал должен храниться безопасным способом, и должно быть зафиксировано лицо, нашедшее документ, место и время нахождения документа и свидетели находки; любое исследование должно удостоверить, что оригиналы не подделаны;

b) для информации на компьютерных носителях: зеркальное отображение или копии (в зависимости от применимых требований) любых сменных носителей, информации на жестких дисках или основной памяти компьютера следует выполнять таким образом, чтобы обеспечить доступность; журнал регистрации всех действий в течение процесса копирования необходимо сохранить, а сам процесс копирования удостоверить; оригиналы носителей информации и журнал регистрации (если это не представляется возможным, то, по крайней мере, один зеркальный образ или копию) следует хранить надежно и без изменений.

Любое судебное разбирательство должно проводиться только по копиям доказательного материала. Целостность доказательного материала необходимо защищать. Копирование доказательного материала должно контролироваться заслуживающим доверия персоналом, а информация о том, когда и где осуществлялся процесс копирования, кто этим занимался и какие инструментальные средства и программы были использованы, должна регистрироваться.

Дополнительная информация

Когда событие информационной безопасности обнаруживаются впервые, не очевидно, приведет ли оно к судебным разбирательствам или нет. Поэтому существует опасность того, что необходимое доказательство будет уничтожено преднамеренно или случайно прежде, чем будет осознана серьезность инцидента. Целесообразно на самом раннем этапе привлечь юриста или полицию в любом случае предполагаемых судебных разбирательств, и получить консультацию относительно требуемых доказательств.

Доказательство может выходить за границы организации и (или) юрисдикции. В таких случаях, следует обеспечивать уверенность в том, что организация имеет право сбора необходимой информации в качестве доказательства. Необходимо также учитывать требования различных юрисдикций, чтобы максимально увеличить шанс признания доказательства в рамках соответствующих юрисдикций.

14 Менеджмент непрерывности бизнеса

14.1 Аспекты информационной безопасности в рамках менеджмента непрерывности бизнеса

Цель: Противодействовать прерываниям видов деятельности в рамках бизнеса организации и защищать важнейшие процессы бизнеса от последствий значительных сбоев информационных систем или чрезвычайных ситуаций и обеспечивать их своевременное возобновление.

Необходимо внедрить процесс менеджмента непрерывности бизнеса с целью минимизации негативного влияния на организацию и восстановления после потери информационных активов (которые могут быть результатом, например стихийных бедствий, несчастных случаев, отказов оборудования и преднамеренных действий) до приемлемого уровня с помощью комбинирования профилактических и восстановительных мер и средств контроля и управления. Указанный процесс должен выявлять критические процессы бизнеса и объединять требования к менеджменту информационной безопасности в части непрерывности бизнеса с другими требованиями по обеспечению непрерывности, касающимися функционирования, кадрового обеспечения, складского хозяйства, транспорта и оборудования.

Последствия стихийных бедствий, нарушений безопасности, отказов в обслуживании и потери доступности обслуживания необходимо анализировать на предмет их влияния на бизнес. Необходимо разработать и внедрить планы обеспечения непрерывности бизнеса с целью обеспечения уверенности в том, что значимые операции могут быть возобновлены в течение требуемого времени. Информационная безопасность должна стать составной частью всего процесса обеспечения непрерывности бизнеса и других процессов менеджмента, реализуемых в организации.

Необходимо, чтобы менеджмент непрерывности бизнеса включал в себя меры и средства контроля и управления по выявлению и снижению рисков в дополнение к общему процессу оценки рисков, ограничения последствий разрушительных инцидентов и обеспечения уверенности в том, что информация, требуемая для процессов бизнеса, легко доступна.

14.1.1 Включение информационной безопасности в процесс менеджмента непрерывности бизнеса

Мера и средство контроля и управления

Следует разрабатывать и поддерживать управляемый процесс для обеспечения непрерывности бизнеса во всей организации, который учитывает требования к информационной безопасности, необходимые для обеспечения непрерывности бизнеса организации.

Рекомендация по реализации

Данный процесс должен объединять следующие ключевые элементы менеджмента непрерывности бизнеса:

a) понимание рисков, с которыми сталкивается организация, с точки зрения вероятности и продолжительности воздействия, включая определение критических процессов бизнеса и установление их приоритетов (см. 14.1.2);

b) определение всех активов, вовлеченных в критические процессы бизнеса (см. 7.1.1);

c) понимание последствий для бизнеса, которые могут быть вызваны прерываниями, обусловленными инцидентами информационной безопасности (важно, чтобы были найдены решения, которые будут применяться как в случае незначительных, так и существенных инцидентов, потенциально угрожающих жизнедеятельности организации), а также определение целей бизнеса применительно к средствам обработки информации;

d) рассмотрение возможности подходящего страхования, которое может стать частью общего процесса непрерывности бизнеса, а также частью менеджмента эксплуатационного риска;

e) определение и рассмотрение внедрения дополнительных превентивных и нейтрализующих мер и средств контроля и управления;

f) определение достаточности финансовых, организационных, технических ресурсов и ресурсов окружающей среды для реагирования на выявленные требования информационной безопасности;

g) обеспечение безопасности персонала и защита средств обработки информации и имущества организации;

h) разработку и документальное оформление планов обеспечения непрерывности бизнеса, учитывающих требования информационной безопасности в соответствии с согласованной стратегией обеспечения непрерывности бизнеса (см. 14.1.3);

i) регулярное тестирование и обновление данных планов и применяемых процессов (см. 14.1.5);

j) обеспечение уверенности в том, что менеджмент непрерывности бизнеса органично вписывается в процессы и структуру организации; ответственность за процесс менеджмента информационной безопасности следует назначать на соответствующем уровне в рамках организации (см. 6.1.1).

14.1.2 Непрерывность бизнеса и оценка риска

Мера и средство контроля и управления

События, которые могут стать причиной прерываний процессов бизнеса, необходимо определять вместе с вероятностью и влиянием таких прерываний, а также их последствиями для информационной безопасности.

Рекомендация по реализации

Необходимо, чтобы аспекты информационной безопасности в контексте обеспечения непрерывности бизнеса основывались на выявлении событий (или последовательности событий), которые могут стать причиной прерываний бизнес-процессов организаций, например отказ оборудования, ошибки оператора, кража, пожар, стихийные бедствия и терроризм. Данный процесс должен сопровождаться оценкой рисков с целью определения вероятности и последствий указанных прерываний с точки зрения времени, масштаба повреждения и периода восстановления.

Оценки рисков в отношении непрерывности бизнеса необходимо осуществлять при непосредственном участии владельцев ресурсов бизнеса и процессов. Данная оценка должна охватывать все процессы бизнеса и не ограничиваться средствами обработки информации, но она должна учитывать результаты, относящиеся к информационной безопасности. Важно объединить различные аспекты риска, чтобы получить полную картину требований организации в отношении непрерывности бизнеса. Оценка должна идентифицировать риски, определять их количество и приоритет по отношению к критериям и целям, имеющим значение для организации, включая критические ресурсы, последствия нарушений, допустимое время простоя и приоритеты восстановления.

В зависимости от результатов оценки рисков, необходимо разработать стратегию, чтобы определить общий подход к обеспечению непрерывности бизнеса. После того как эта стратегия будет разработана, необходимо, чтобы она была утверждена руководством, а также, чтобы был разработан и утвержден план реализации данной стратегии.

14.1.3 Разработка и внедрение планов обеспечения непрерывности бизнеса, учитывающих информационную безопасность

Мера и средство контроля и управления

Следует разработать и внедрить планы обеспечения непрерывности бизнеса с целью поддержки или восстановления операций и обеспечения доступности информации на требуемом уровне и в требуемые сроки после прерывания или сбоя критических процессов бизнеса.

Рекомендация по реализации

Процесс планирования непрерывности бизнеса должен предусматривать следующее:

a) определение и согласование всех обязанностей и процедур, связанных с обеспечением непрерывности бизнеса;

b) определение приемлемых потерь информации и услуг;

c) внедрение процедур, позволяющих восстановить и возобновить операции бизнеса и доступность информации в требуемые сроки; особое внимание следует уделить оценке внешних и внутренних зависимостей бизнеса и существующих договоров;

d) эксплуатационные процедуры, которым необходимо следовать в ожидании завершения восстановления и возобновления;

e) документальное оформление согласованных процедур и процессов;

f) соответствующее обучение сотрудников согласованным процедурам и процессам, включая управление в критических ситуациях;

g) тестирование и обновление планов.

Необходимо, чтобы в процессе планирования особое внимание было обращено на требуемые цели бизнеса, например восстановление определенных услуг связи для клиентов в приемлемые сроки. Следует учитывать потребность в необходимых для этого услугах и ресурсах, включая укомплектованность персоналом, ресурсы, не связанные с обработкой информации, а также меры по переходу на аварийный режим средств обработки информации. Такие меры по переходу на аварийный режим могут включать в себя договоренности с третьей стороной в виде взаимных соглашений или коммерческих абонируемых услуг.

Планы обеспечения непрерывности бизнеса должны учитывать уязвимости организации и поэтому могут содержать чувствительную информацию, нуждающуюся в соответствующей защите. Копии планов обеспечения непрерывности бизнеса следует хранить на достаточном расстоянии от основного здания, чтобы избежать их повреждения вследствие аварии в основном здании. Руководство должно обеспечить уверенность в том, что обновление и защита планов обеспечения непрерывности бизнеса осуществляется на том же уровне, что и в основном здании. Другие материалы, необходимые для выполнения планов по обеспечению непрерывности бизнеса, следует также хранить в удаленном месте.

Если для хранения используются различные врéменные помещения, то уровень реализуемых мер и средств контроля и управления безопасности в таких помещениях должен соответствовать уровню мер, реализуемых в основном здании.

Дополнительная информация

Следует заметить, что планы по управлению в критических ситуациях и действия, (см. перечисление f) в 14.1.3) могут отличаться от менеджмента непрерывности бизнеса, т. е. кризис может быть улажен обычными процедурами управления.

14.1.4 Основы планирования непрерывности бизнеса

Мера и средство контроля и управления

Следует поддерживать единую структуру планов непрерывности бизнеса, чтобы обеспечить уверенность в том, что все планы согласованы в соответствии с рассматриваемыми требованиями информационной безопасности и установленными приоритетами для тестирования и обслуживания.

Рекомендация по реализации

В каждом плане обеспечения непрерывности бизнеса должен описываться подход к обеспечению непрерывности, например подход к обеспечению уверенности в доступности и безопасности информации или информационных систем. Каждый план должен определять план эскалации (расширения) и условия активизации, а также лиц, ответственных за выполнение каждого пункта плана. При появлении новых требований любые существующие процедуры на случай чрезвычайных ситуаций, например планы эвакуации или меры по переходу на аварийный режим, при необходимости следует корректировать. Процедуры должны быть включены в программу менеджмента изменений организации с целью обеспечения уверенности в том, что вопросы обеспечения непрерывности бизнеса рассматриваются всегда соответствующим образом.

Каждый план должен иметь определенного владельца. Процедуры на случай чрезвычайных ситуаций, планы по переходу на аварийный режим, планы по возобновлению следует включать в сферу ответственности владельцев соответствующих ресурсов бизнеса или вовлеченных процессов. Ответственность за меры по переходу на аварийный режим альтернативных технических услуг, таких как обработка информации и средства связи, обычно несут поставщики услуг.

В основу планирования непрерывности бизнеса должны быть заложены требования информационной безопасности, и предусмотрено следующее:

a) условия активизации планов, описывающие процесс, которому необходимо следовать (например как оценить ситуацию, кто должен принимать участие), прежде чем привести в действие каждый план;

b) процедуры, определяющие порядок действий при чрезвычайных ситуациях, которые должны быть предприняты после инцидента, ставящего под угрозу операции бизнеса;

c) процедуры перехода на аварийный режим, описывающие действия, которые должны быть предприняты, чтобы перенести важные операции бизнеса и услуги поддержки в альтернативное врéменное место размещения и восстановить процессы бизнеса в требуемые сроки;

d) врéменные эксплуатационные процедуры, которых следует придерживаться в ожидании завершения восстановления и возобновления;

e) процедуры возобновления, определяющие порядок действий, которые должны быть предприняты, чтобы вернуться к нормальному состоянию операций бизнеса;

f) график поддержки плана, который определяет способ и время проверки, а также процесс поддержки плана в актуальном состоянии;

g) информирование, обучение и тренинг, направленные на понимание процессов обеспечения непрерывности бизнеса и обеспечение уверенности в эффективности этих процессов;

h) обязанности лиц с указанием ответственных за выполнение каждого пункта плана, при необходимости должны быть указаны альтернативные ответственные лица;

i) важнейшие активы и ресурсы, необходимые для действий в чрезвычайных ситуациях, при переходе на аварийный режим и в процедурах возобновления.

14.1.5 Тестирование, поддержка и пересмотр планов непрерывности бизнеса

Мера и средство контроля и управления

Планы непрерывности бизнеса необходимо регулярно тестировать и обновлять с целью обеспечения уверенности в их актуальности и эффективности.

Рекомендация по реализации

Указанные тесты должны обеспечивать уверенность в том, что все члены группы ликвидации последствий чрезвычайных ситуаций и другой персонал, имеющий к этому отношение, осведомлены о планах и о своих обязанностях, касающихся обеспечения непрерывности бизнеса и информационной безопасности.

В графике тестирования плана(ов) по обеспечению непрерывности бизнеса необходимо указывать, как и когда следует тестировать каждый пункт плана. Отдельные пункты плана(ов) необходимо тестировать часто.

Следует использовать различные методы для обеспечения уверенности в том, что план(ы) будет(ут) действовать в реальной жизни. К таким методам относятся:

a) теоретическая проверка различных сценариев (обсуждение мер по восстановлению бизнеса на различных примерах прерываний);

b) моделирование особенно для тренинга сотрудников по выполнению их ролей менеджмента в постинцидентных и кризисных ситуациях;

c) тестирование технического восстановления (обеспечение уверенности в возможности эффективного восстановления систем);

d) тестирование процессов восстановления деятельности на альтернативной площадке (процессы бизнеса осуществляются параллельно с процедурами восстановления на удаленной альтернативной площадке);

e) тестирование оборудования и услуг поставщиков (обеспечение уверенности в том, что предоставленные сторонними организациями продукты и услуги удовлетворяют договорным обязательствам);

f) «генеральные репетиции» (проверка готовности персонала, оборудования, средств и процессов к обеспечению непрерывности бизнеса).

Указанные методы могут использоваться любой организацией. Они должны применяться в соответствии со спецификой конкретного плана по восстановлению. Результаты тестов следует регистрировать и при необходимости осуществлять действия, направленные на совершенствование планов.

Необходимо назначить ответственных за проведение регулярных пересмотров каждого плана по обеспечению непрерывности бизнеса. Выявление изменений в процессах бизнеса, еще не отраженных в планах по обеспечению непрерывности бизнеса, должно сопровождаться соответствующим обновлением планов. Указанный формальный процесс управления изменениями призван обеспечить уверенность в том, что обновленные планы распространяются и подкрепляются в соответствии с регулярным пересмотром комплексного плана.

Примеры ситуаций, которые могли бы потребовать обновления планов по обеспечению непрерывности бизнеса, включают приобретение нового оборудования или обновления систем, а также изменения, связанные с:

a) персоналом;

b) адресами или номерами телефонов;

c) стратегией бизнеса;

d) местоположением, условиями и ресурсами;

e) законодательством;

f) подрядчиками, поставщиками и основными клиентами;

g) процессами, как новыми, так упраздненными;

h) рисками (эксплуатационными и финансовыми).

15 Соответствие

15.1 Соответствие требованиям законодательства

Цель: Избежать нарушений любого закона, правовых, нормативных или договорных обязательств, а также любых требований безопасности.

Проектирование, функционирование, использование информационных систем и управление ими может быть предметом применения правовых, нормативных и договорных требований безопасности.

Следует консультироваться с юристами организации в отношении конкретных юридических вопросов, или с практикующими юристами, имеющими соответствующую квалификацию. Законодательные требования разных стран отличаются друг от друга, и они могут меняться в отношении информации, созданной в одной стране и переданной в другую страну (например информационный поток, передаваемый через границу).

15.1.1 Определение применимого законодательства

Мера и средство контроля и управления

Все применимые правовые, нормативные и договорные требования и подход организации к выполнению этих требований следует четко определить, документально оформить и поддерживать на актуальном уровне в отношении каждой информационной системы и организации.

Рекомендация по реализации

Конкретные меры и средства контроля и управления, а также обязанности конкретных лиц по выполнению этих требований необходимо определить и документально оформить.

15.1.2 Права на интеллектуальную собственность

Мера и средство контроля и управления

Необходимо внедрить соответствующие процедуры для обеспечения уверенности в соблюдении законодательных, нормативных и договорных требований по использованию материалов, в отношении которых могут иметься права на интеллектуальную собственность, и по использованию проприетарных[1)] программных продуктов.

Рекомендация по реализации

Следующие рекомендации следует учитывать в отношении защиты любого материала, который может рассматриваться как интеллектуальная собственность:

a) создание политики соблюдения прав на интеллектуальную собственность в отношении программного обеспечения, определяющей законное использование программных и информационных продуктов;

b) приобретение программного обеспечения только из известных и заслуживающих доверия источников для обеспечения уверенности в том, что авторское право не нарушается;

c) поддержание осведомленности сотрудников о политиках по защите прав на интеллектуальную собственность и уведомление о намерении применить дисциплинарные санкции в отношении нарушителей;

d) поддержание соответствующих реестров активов и выявление всех активов, в отношении которых применимы требования по защите прав на интеллектуальную собственность;

e) сохранение подтверждений и свидетельств прав собственности на лицензии, дистрибутивные диски, руководства по эксплуатации и т. д.;

f) внедрение мер и средств контроля и управления для обеспечения уверенности в том, что максимальное число разрешенных пользователей не превышено;

g) проведение проверок на предмет установки только авторизованного программного обеспечения и лицензированных продуктов;

h) предоставление политики по поддержке условий соответствующих лицензионных соглашений;

i) предоставление политики утилизации или передачи программного обеспечения другим сторонним организациям;

j) использование соответствующих инструментальных средств аудита;

[1)] Проприетарное программное обеспечение:

1) программное обеспечение защищённое авторским/патентным правом. Модификация и дальнейшее распространение такого программного обеспечения запрещена или строго ограничена;

2) программы собственного производства, разработанные компаниями для внутреннего использования (в отличие от стандартных программных средств известных производителей).

k) соблюдение сроков и условий применения программного обеспечения и информации, полученной из общедоступных сетей;

l) запрещать дублирование, преобразование или извлечение из коммерческих записей (видео, аудио) с нарушением закона об авторском праве;

m) запрещать полное или частичное копирование книг, статей, отчетов или других документов с нарушением закона об авторском праве.

Дополнительная информация

Права на интеллектуальную собственность охватывают авторское право на программное обеспечение или документы, права на проекты, торговые марки, патенты и лицензии на исходные тексты программ.

Проприетарные программные продукты обычно поставляются в соответствии с лицензионным соглашением, которое определяет права по срокам и условиям использования, например ограничение на использование продуктов в указанных компьютерах или ограничение копирования только созданием резервных копий. Ситуацию в отношении прав на интеллектуальную собственность в отношении программного обеспечения, разработанного организацией, следует разъяснить персоналу.

Законодательные, нормативные и договорные требования могут вводить ограничения на копирование материалов, являющихся предметом собственности. В частности, данные ограничения могут содержать требования на использование только тех материалов, которые или разработаны организацией, или представлены по лицензии, или переданы разработчикам для организации. Нарушение авторского права может привести к судебному иску, который может повлечь уголовное преследование.

15.1.3 Защита документов организации

Мера и средство контроля и управления

Важные документы организации необходимо защищать от потери, разрушения и фальсификации в соответствии с законодательными, нормативными и договорными требованиями, а также требованиями бизнеса.

Рекомендация по реализации

Документы необходимо классифицировать по типам, например бухгалтерские счета, записи баз данных, журналы регистрации транзакций, контрольные журналы и методики эксплуатации, с указанием периода хранения и типа носителей хранимых данных, например бумага, микрофиша[1)], магнитные и оптические носители. Любые данные, связанные с криптографическими ключами и программы, связанные с зашифрованными архивами или цифровыми подписями (см. 12.3), следует также хранить для обеспечения возможности дешифрования записей в течение всего времени их хранения.

Необходимо учитывать возможность снижения качества носителей, используемых для хранения документов. Процедуры хранения и обращения с носителями должны осуществляться в соответствии с рекомендациями изготовителя. При необходимости долгосрочного хранения рекомендуется использование бумаги и микрофишей.

Там, где для хранения используются электронные носители данных, следует применять процедуры, обеспечивающие уверенность в возможности доступа к данным (читаемость носителей 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 в приемлемые сроки и в приемлемом формате в зависимости от требований.

Система хранения должна обеспечивать четкую идентификацию документов, а также период их хранения, установленный соответствующими национальными или региональными законами или нормами. Необходимо, чтобы эта система предоставляла возможность уничтожения документов после того, как у организации отпадет потребность в их хранении.

Чтобы реализовать эти требования по защите документов, организации необходимо предпринимать следующее:

a) разработать рекомендации в отношении сроков, порядка хранения и обработки, а также уничтожения документов и информации;

b) составить график хранения с указанием документов и периода, в течение которого их необходимо хранить;

c) поддерживать ведение учета источников ключевой информации;

[1)] Микрофиша — пленка или пластина с несколькими десятками кадров микрофильма. Микрофиши имеют стандартные размеры под устройства их изготовления и просмотра. Эта технология широко использовалась в 1970—1980-е годы, а затем была вытеснена компьютерными носителями данных.

d) необходимо внедрить соответствующие меры и средства контроля и управления с целью защиты документов и информации от потери, разрушения и фальсификации.

Дополнительная информация

В отношении некоторых документов может потребоваться обеспечение безопасного хранения с целью выполнения законодательных, нормативных и договорных требований, а также для поддержки бизнеса. Например документы, которые могут потребоваться как доказательство того, что организация работает в рамках установленных законодательных и нормативных правил, чтобы обеспечить адекватную защиту от потенциального гражданского или уголовного преследования, или для подтверждения финансового состояния организации, касающегося акционеров, внешних сторон и аудиторов. Период времени и содержание данных для сохранения информации могут устанавливаться национальными законами или нормами.

Более подробную информацию о менеджменте документов организации можно найти в ИСО 15489-1 [12].

15.1.4 Защита данных и конфиденциальность персональных данных

Мера и средство контроля и управления

Должна быть обеспечена уверенность в защите данных и персональных данных в соответствии с требованиями соответствующих законодательных и нормативных актов и, в случае необходимости, условий договоров.

Рекомендация по реализации

Необходимо разработать и внедрить политику организации в отношении обеспечения защиты данных и персональных данных. Эта политика должна быть доведена до сведения всех лиц, участвующих в обработке персональной информации.

Соблюдение указанной политики и всех применимых требований законодательных и нормативных актов по защите данных подразумевает наличие соответствующей структуры управления и контроля. Часто это лучше всего достигается путем назначения ответственного лица, например должностного лица, отвечающего за защиту данных, которое должно предоставить инструкции руководителям среднего звена, пользователям и поставщикам услуг в отношении их персональной ответственности и специальных процедур, обязательных для выполнения. Обеспечение ответственности за обработку персональной информации и осведомленности о принципах защиты данных должно осуществляться в соответствии с требованиями применимых законодательных и нормативных актов. В целях защиты персональной информации следует реализовать соответствующие технические и организационные меры.

Дополнительная информация

В ряде стран введены законодательные нормы, устанавливающие меры и средства контроля и управления в отношении сбора, обработки и передачи персональных данных (в основном, это касается информации о людях, которые могут быть идентифицированы по этой информации).

В зависимости от соответствующего национального законодательства, такие меры и средства контроля и управления могут возлагать определенные обязанности на тех, кто осуществляет сбор, обработку и распространение персональной информации, а также могут ограничить возможность передачи указанных данных в другие страны.

15.1.5 Предотвращение нецелевого использования средств обработки информации

Мера и средство контроля и управления

Пользователей следует удерживать от применения средств обработки информации для несанкционированных целей.

Рекомендация по реализации

Руководство должно санкционировать использование средств обработки информации. Любое использование этих средств для непроизводственных целей без одобрения руководства (см. 6.1.4) или для каких-либо несанкционированных целей следует рассматривать как нецелевое. Если какие-либо несанкционированные действия определяются мониторингом или другими средствами, то на них следует обратить внимание непосредственного руководителя сотрудника, с целью принятия соответствующих мер дисциплинарного и (или) правового воздействия.

Прежде чем осуществлять процедуры мониторинга, необходимо получить консультацию юриста.

Все пользователи должны быть осведомлены о четких рамках разрешенного им доступа и о проведении мониторинга с целью обнаружения несанкционированного использования средств обработки информации. Это может быть достигнуто путем предоставления пользователям письменного разрешения, копия которого должна быть подписана пользователем и надежно храниться в организации. Необходимо, чтобы сотрудники организации, подрядчики и представители сторонней организации были осведомлены о том, что никакой доступ не разрешен, за исключением того, который авторизован.

Необходимо, чтобы при начале сеанса на экране компьютера было представлено предупреждающее сообщение, указывающее, что средство обработки информации, вход в которое пытаются осуществить, является собственностью организации, и что несанкционированный доступ к нему запрещен. Пользователь должен подтвердить прочтение и соответствующим образом реагировать на это сообщение на экране, чтобы продолжить процесс начала сеанса (см. 11.5.1).

Дополнительная информация

Средства обработки информации организации должны использоваться главным образом или только для решения задач бизнеса.

Обнаружение вторжения, проверка содержания и другие средства мониторинга могут помочь в предотвращении и обнаружении нецелевого использования средств обработки информации.

Во многих странах введено законодательство, касающееся защиты от неправильного использования компьютеров. Использование компьютера для несанкционированных целей может расцениваться как уголовное преступление.

Законность проведения мониторинга в отношении использования средств обработки информации зависит от страны, и может потребоваться, чтобы сотрудники были уведомлены о таком мониторинге и (или) чтобы было получено их согласие. При осуществлении входа в систему, используемую для открытого доступа (например общественный Web-сервер) и подвергаемую мониторингу безопасности, на экране компьютера должно отображаться сообщение, информирующее об этом.

15.1.6 Регулирование криптографических мер и средств контроля и управления

Мера и средство контроля и управления

Криптографические меры и средства контроля и управления должны использоваться с соблюдением всех соответствующих соглашений, законов и нормативных актов.

Рекомендация по реализации

Следующие вопросы необходимо рассматривать в отношении соблюдения соответствующих соглашений, законов и нормативных актов:

a) ограничения на импорт и (или) экспорт компьютерных аппаратных и программных средств для выполнения криптографических функций;

b) ограничения на импорт и (или) экспорт компьютерных аппаратных и программных средств, которые разработаны таким образом, что имеют в качестве дополнения криптографические функции;

c) ограничения на использование шифрования;

d) обязательные или представленные по собственному усмотрению методы доступа государственных органов к информации, зашифрованной с помощью аппаратных или программных средств для обеспечения конфиденциальности содержания.

С целью обеспечения уверенности в соответствии национальным законам и нормативным актам, необходимо обратиться за консультацией к юристу. Прежде чем зашифрованная информация или криптографическое средство будут переданы другой стране, необходимо также получить консультацию юриста.

15.2 Соответствие политикам безопасности и стандартам, техническое соответствие

Цель: Обеспечить уверенность в соответствии систем политикам безопасности организации и стандартам.

Безопасность информационных систем необходимо регулярно пересматривать.

Такие пересмотры необходимо осуществлять по отношению к соответствующим политикам безопасности, а технические платформы и информационные системы должны подвергаться проверке на предмет соответствия применимым стандартам безопасности и документированным мерам и средствам контроля и управления безопасности.

15.2.1 Соответствие политикам и стандартам безопасности

Мера и средство контроля и управления

Руководители должны обеспечить уверенность в том, что все процедуры безопасности в пределах их зоны ответственности выполняются правильно, для того чтобы достичь соответствия политикам и стандартам безопасности.

Рекомендация по реализации

Руководители должны регулярно анализировать соответствие обработки информации в пределах их зоны ответственности политикам и стандартам безопасности, а также любым другим требованиям безопасности.

Если в результате проведения анализа было выявлено какое-либо несоответствие, руководителям следует:

a) определить причины несоответствия;

b) оценить необходимость действий с целью обеспечения уверенности в том, что несоответствие не повторится;

c) определить и реализовать соответствующее корректирующее действие;

d) проанализировать предпринятое корректирующее действие.

Результаты анализа и корректирующих действий, предпринятых руководителями, необходимо регистрировать, и эти записи следует сохранять. Руководители должны сообщать результаты лицам, проводящим независимые проверки (см. 6.1.8), если такая независимая проверка имела место в зоне их ответственности.

Дополнительная информация

Мониторинг использования систем рассмотрен в 10.10.

15.2.2 Проверка технического соответствия

Мера и средство контроля и управления

Информационные системы следует регулярно проверять на соответствие применимым стандартам безопасности.

Рекомендация по реализации

Проверку соответствия техническим требованиям должен осуществлять опытный системный инженер вручную (при необходимости с помощью соответствующих инструментальных средств программного обеспечения) и (или) с помощью автоматизированных инструментальных средств, которые генерируют технический отчет для последующего анализа техническим специалистом.

Если проводится тестирование на проникновение или оценка уязвимостей, следует соблюдать осторожность, поскольку такие действия могут привести к компрометации безопасности системы. Такие тесты должны быть спланированы, документально оформлены и воспроизводимы.

Любая проверка соответствия техническим требованиям должна выполняться только компетентными и уполномоченными лицами либо под их наблюдением.

Дополнительная информация

Проверка соответствия техническим требованиям включает обследование эксплуатируемых систем на предмет обеспечения уверенности в том, что аппаратные и программные средства управления были правильно реализованы. Этот тип проверки соответствия требует специальных технических знаний.

Проверка соответствия также охватывает, например тестирование на проникновение и оценку уязвимостей, которые могут быть выполнены независимыми экспертами, привлекаемыми на контрактной основе специально для этой цели. Это может быть полезным для обнаружения уязвимостей в системе и для проверки того, насколько эффективны меры и средства контроля и управления, направленные на предотвращение несанкционированного доступа, возможного вследствие этих уязвимостей.

Тестирование на проникновение и оценка уязвимостей дают возможность получить «стоп-кадр» системы в определенном состоянии и в определенное время. «Стоп-кадр» ограничивается теми частями системы, которые фактически тестируются во время попытки(ок) осуществления проникновения. Тестирование на проникновение и оценка уязвимостей не заменяют оценку рисков.

15.3 Рассмотрение аудита информационных систем

Цель: Повышение до максимума эффективности процесса аудита информационных систем и снижение до минимума негативного влияния, связанного с данным процессом.

Необходимо наличие мер и средств контроля и управления для защиты эксплуатируемых систем и инструментальных средств аудита в процессе проведения аудита информационных систем.

Также необходимо принять меры для защиты целостности и предотвращения неправильного использования инструментальных средств аудита.

15.3.1 Меры и средства контроля и управления аудита информационных систем

Мера и средство контроля и управления

Требования и процедуры аудита, включающие проверки эксплуатируемых систем, необходимо тщательно планировать и согласовывать, чтобы свести к минимуму риск нарушения процессов бизнеса.

Рекомендация по реализации

Необходимо учитывать следующие рекомендации:

a) требования аудита должны быть согласованы с соответствующим руководством;

b) область проверок следует согласовывать и контролировать;

c) при проведении проверок доступ к программному обеспечению и данным должен быть ограничен только чтением;

d) другие виды доступа, кроме доступа только для чтения, могут быть разрешены только в отношении изолированных копий файлов системы, которые необходимо удалить по завершению аудита или обеспечить соответствующей защитой, если необходимо хранить такие файлы в соответствии с требованиями документального оформления аудита;

e) ресурсы, необходимые для выполнения проверок, должны быть четко определены и сделаны доступными;

f) требования в отношении специальной или дополнительной обработки данных следует определить и согласовать;

g) весь доступ необходимо отслеживать и регистрировать для создания прослеживаемых ссылок; для критически важных данных и систем надлежит рассматривать использование датируемых прослеживаемых ссылок;

h) все процедуры, требования и обязанности следует оформлять документально;

i) лицо(а), проводящее(ие) аудит, должно(ы) быть независимым(и).

15.3.2 Защита инструментальных средств аудита информационных систем

Мера и средство контроля и управления

Доступ к инструментальным средства, применяемым при проведении аудита информационных систем, необходимо защищать, чтобы предотвратить любое возможное их неправильное использование или компрометацию.

Рекомендация по реализации

Инструментальные средства, применяемые при проведении аудита информационных систем, например программное обеспечение или файлы данных, необходимо отделять от систем разработки и эксплуатируемых систем, а также, если не обеспечен соответствующий уровень дополнительной защиты, их не следует хранить в библиотеках на магнитных лентах или в области пользователей.

Дополнительная информация

Если к проведению аудита привлечены третьи стороны, то может возникнуть риск неправильного использования инструментальных средств аудита этими третьими сторонами и информации, доступной организации, представляющей третью сторону. Для решения вопросов, связанных с таким риском, могут применяться меры и средства контроля и управления, изложенные в 6.2.1 (для оценки рисков) и 9.2.1 (для ограничения физического доступа), а также иные последующие действия, например незамедлительная смена паролей, открытых для аудиторов.

Библиография

[1] ISO/IEC Guide 2:1996, Standardization and related activities — General vocabulary.

[2] ISO/IEC Guide 73:2002, Risk management — Vocabulary — Guidelines for use in standards.

[3] ISO/IEC 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management.

[4] ISO/IEC TR 13335-3:1998, Information technology — Guidelines for the Management of IT Security — Part 3: Techniques for the management of IT Security.

[5] ISO/IEC 13888-1:1997, Information technology — Security techniques — Non-repudiation — Part 1: General.

[6] ISO/IEC 11770-1:1996 Information technology — Security techniques — Key management — Part 1: Framework *(ИСО/МЭК 11770-1:1996 Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент ключей. Часть 1. Структура)* *.

[7] ISO/IEC 9796-2:2002 Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms.

[8] ISO/IEC 9796-3:2000 Information technology — Security techniques — Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms.

[9] ISO/IEC 14888-1:1998 Information technology — Security techniques — Digital signatures with appendix — Part 1: General.

[10] ISO/IEC 15408-1:1999 Information technology — Security techniques — Evaluation Criteria for IT security — Part 1: Introduction and general model.

[11] ISO/IEC 14516:2002 Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services.

[12] ISO 15489-1:2001 Information and documentation — Records management — Part 1: General *(ИСО/МЭК 15489-1:2001 Информация и документация. Управление записями. Часть 1. Общие требования)* *.

[13] ISO 10007:2003 Quality management systems — Guidelines for configuration management.

[14] ISO/IEC 12207:1995 Information technology — Software life cycle processes.

[15] ISO 19011:2002 Guidelines for quality and /or environmental management systems auditing.

[16] OECD Guidelines for the Security of Information Systems and Networks: 'Towards a Culture of Security', 2002.

[17] OECD Guidelines for Cryptography Policy, 1997.

[18] IEEE P1363-2000: Standard Specifications for Public-Key Cryptography.

[19] ISO/IEC 18028-4 Information technology — Security techniques — IT Network security — Part 4: Securing remote access.

[20] ISO/IEC TR 18044 Information technology — Security techniques — Information security incident management *(ИСО/МЭК ТО 18044 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности)* *.

---

* Официальный перевод этого международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Указатель

A

access control (управление доступом) 11
— for application systems (к прикладным систем) 11.6
— business requirements for (требования бизнеса по) 11.1
— for information (к информации) 11.6, 11.6.1
— for networks (к сети) 11.4
— for operating systems (к эксплуатируемой системе) 11.5
— policy for (политика по) 11.1.1
— to program source code (к исходным текстам программ) 12.4.3
access rights (права доступа)
— removal of (аннулирование) 8.3.3
— review of (пересмотр) 11.2.4
acceptable use of assets (приемлемое использование активов) 7.1.3
accountability (подотчетность) 2.5
acquisition, development and maintenance of information systems (приобретение, разработка и эксплуатация информационных систем) 12
agreements (соглашения/договоры)
— addressing security in third party (рассмотрение требований безопасности с третьей стороной) 6.2.3
— for exchange (по обмену) 10.8.2
allocation of information security responsibilities (распределение обязанностей по обеспечению информационной безопасности) 6.1.3
application (прикладная программа)
— correct processing in applications (корректная обработка в прикладных программах) 12.2
— review of, after operating system changes (проверка после изменений эксплуатируемой системы) 12.5.2
— system access control (управление доступом к системе) 11.6
asset (актив) 2.1
— acceptable use of (приемлемое использование) 7.1.3
— inventory of (инвентаризация) 7.1.1
— management (менеджмент) 7
— ownership of (владение) 7.1.2
— responsibility for (ответственность за) 7.1
— return of (возврат) 8.3.2
audit (аудит)
— considerations for information systems (рассмотрение информационных систем) 15.3
— controls for information systems (меры и средства контроля и управления информационных систем) 15.3.1
— logging (регистрация) 10.10.1
— tools, protection of (инструментальные средства, защита) 12.3.2
authentication (аутентификация)
— of users (пользователей) 11.5.2
— of users for external connections (пользователей для внешних соединений) 11.4.3
authenticity (аутентичность) 2.5
authorities, contact with (инстанции, контакты с) 6.1.6
authorization process (процесс получения разрешения) 6.1.4
availability (доступность) 2.5
awareness, education and training in information security (осведомленность, обучение и тренинг в области информационной безопасности) 8.2.2

B

back-up (резервирование) 10.5
— of information (информации)10.5.1
business continuity (непрерывность бизнеса) 14
— management of (менеджмент) 14
— management of information security aspects of (аспекты информационной безопасности в рамках менеджмента) 14.1
— management process to include information security in (включение информационной безопасности в процесс менеджмента) 14.1.1
— planning, framework for (планирование, структура по) 14.1.4

— plans, development and implementation (планы, разработка и внедрение) 14.1.3
— and risk assessment (и оценка риска) 14.1.2
— testing, maintaining and re-assessing plans for (тестирование, поддержка и пересмотр планов) 14.1.5
business information systems (информационные системы бизнеса) 10.8.5

C

cabling security (безопасность кабельной сети) 9.2.3
capacity management (управление производительностью) 10.3.1
change (изменение)
— control, procedures for (управление, процедуры по) 12.5.1
— of employment (занятости) 8.3
— management (менеджмент) 10.2.1
— of operating systems, review of (эксплуатируемых систем, изменений) 12.5.2
— restriction of changes to software packages (ограничения на изменения пакетов программ) 12.5.3
changes to third party services, management of (изменениями услуг третьей стороны, управление) 10.2.3
classification (классификация)
— guidelines (рекомендации) 7.2.1
— of information (информации) 7.2
clear desk and clear screen policy (политика «чистого стола» и «чистого экрана») 11.3.3
clock synchronization (синхронизация часов) 10.10.6
collection of evidence (сбор доказательств) 13.2.3
communications and operations management (менеджмент коммуникаций и работ) 10
compliance (соответствие) 15
— technical compliance checking (проверка технического соответствия) 15.2.2
— with legal requirements (требованиям законодательства) 15.1
— with security policies and standards (политикам безопасности и стандартам) 15.2, 15.2.1
confidentiality (конфиденциальность) 2.5
confidentiality agreements (соглашения о конфиденциальности) 6.1.5
configuration port protection, remote (защита портов конфигурации, диагностики) 11.4.4
connection control of networks (управление сетевыми соединениями) 11.4.6
connection time, limitation of (время соединения, ограничение) 11.5.6
contact (контакт)
— with authorities (с различными инстанциями) 6.1.6
— with specialist interest groups (со специальными группами по интересам) 6.1.7
control (мера и средство контроля и управления) 2.2, 3.2
— against malicious code (против вредоносной программы) 10.4.1
— against mobile code (против мобильной программы) 10.4.2
— of internal processing (внутренней обработкой) 12.2.2
— of operational software (эксплуатируемым программным обеспечением) 12.4.1
copyright (авторское право)
— IPR (право на интеллектуальную собственность) 15.1.2
— software (программа) 15.1.2
correct processing in applications (корректная обработка в прикладных программах) 12.2
cryptographic controls (криптографические меры и средства контроля и управления) 12.3
— policy on the use of (политика использования) 12.3.1
— regulation of (регулирование) 15.1.6
customers, addressing security when dealing with (клиенты, рассмотрение вопросов безопасности при работе с) 6.2.2

D

data protection and privacy of personal information (защита данных и конфиденциальность персональных данных) 15.1.4
delivery area (зоны приемки) 9.1.6
development (разработка)
— and acquisition and maintenance of information systems (приобретение и эксплуатация информационных систем) 12
— and test and operational facilities, separation of (средства тестирования и эксплуатации, отделенные от)
— of software, outsourced (программного обеспечения, аутсорсинг) 12.5.5
— and support processes, security in (и процессах поддержки, безопасность в) 12.5
diagnostic port protection, remote (защита портов дистанционной диагностики и конфигурации) 11.4.4

disciplinary process (дисциплинарный процесс) 8.2.3
disposal (утилизация)
— of equipment (оборудования) 9.2.6
— of media (носителей информации) 10.7.2
documentation, security of system (документация, безопасность системы) 10.7.4
documented operating procedures (документальное оформление эксплуатационных процедур) 10.1.1
during employment (в течение занятости) 8.2
duties, segregation of (обязанности, разделение) 10.1.3

E

education, awareness and training in information security (обучение, осведомленность и тренинг в области информационной безопасности) 8.2.2
electronic (электронная)
— commerce (торговля) 10.9.1
— commerce services (услуги торговли) 10.9
— messaging (сообщения) 10.8.4
employment (занятость)
— during (в течение) 8.2
— prior to (перед) 8.1
— termination or change of (прекращение или смена) 8.3
entry controls (меры и средства контроля и управления входом) 9.1.2
environmental and external threats (внешние угрозы и угрозы со стороны окружающей среды) 9.1.4
environmental and physical security (физическая безопасность и защита от воздействий окружающей среды) 9
equipment (оборудование)
— identification in networks (идентификация в сетях) 11.4.3
— maintenance (техническое обслуживание) 9.2.4
— secure disposal or re-use of (безопасная утилизация или повторное использование) 9.2.6
— security (безопасность) 9.2
— security off-premises (безопасность вне помещений) 9.2.5
— siting and protection of (размещение и защита) 9.2.1
— unattended (оставленное без присмотра) 11.3.2
evidence, collection of (доказательства, сбор) 13.2.3
exchange (обмен)
— agreements (соглашения) 10.8.2
— of information (информации) 10.8
— of information, policies and procedures for (информации, политики и процедуры по) 10.8.1
external and environmental threats (внешние угрозы и угрозы со стороны окружающей среды) 9.1.4
external parties (сторонние организации) 6.2
— identification of risks related to (идентификация рисков, являющихся) 6.2.1

F

fault logging (регистрация неисправности) 10.10.5
framework for business continuity plans (структура планов непрерывности бизнеса) 14.1.4

G

guideline (рекомендация) 2.3

H

human resources security (безопасность, связанная с персоналом) 8
home working (работа на дому)
— security of equipment (безопасность оборудования) 9.2.5
— security of teleworking (безопасность дистанционной работы) 11.7.2

I

identification (идентификация)
— of equipment in networks (оборудования в сетях) 11.4.3
— of users (пользователей) 11.5.2
identification of applicable legislation (определение применимого законодательства) 15.1.1
implementation guidance (рекомендация по реализации) 3.2
independent review of information security (независимая проверка информационной безопасности) 6.1.8
information (информация)

— access, restrictions on (доступ, ограничения на) 11.6.1
— back-up of (резервирование) 10.5.1
— classification (классификация) 7.2
— exchange of (обмен) 10.8
— exchange of, policies and procedures for (обмен, политики и процедуры по) 10.8.1
— handling procedures for (процедуры обработки) 10.7.3
— labeling and handling (маркировка и обработка) 7.2.2
— leakage (утечка) 12.5.4
— made publicly available (сделана общедоступной) 10.9.3
— processing facilities (средства обработки) 2.4
— processing facilities and misuse of them (средства обработки и нецелевое использование их) 15.1.5
— system acquisition, development and maintenance (приобретение, разработка и эксплуатация) 12
— system audit controls (меры и средства контроля и управления аудита информационных систем) 15.3.1
— system audit tools, protection of (инструментальные средства аудита информационных систем, защита) 15.3.2
— systems for business (информационные системы бизнеса) 10.8.5
information security (информационная безопасность) 2.5
— awareness, education and training in (осведомленность, обучение и тренинг в) 8.2.2
— co-ordination of (координация) 6.1.2
— event (событие) 2.6, 13.1
— event, reporting of (событие, оповещение о) 13.1.1
— incident (инцидент) 2.7, 13.2
— incident, learning from (инцидент, извлечение уроков из) 13.2.2
— inclusion in the business continuity management process (включение в процесс менеджмента непрерывности бизнеса) 14.1.1
— inclusion in the development and implementation of business continuity plans (включение в разработку и внедрение планов обеспечения непрерывности бизнеса) 14.1.3
— organizing (организация) 6
— policy for (политика по) 5.1
— policy document for (документирование политики) 5.1.1
input data validation (подтверждение корректности входных данных) 12.2.1
integrity (целостность) 2.5
— of messages (сообщений) 12.2.3
intellectual property rights (права на интеллектуальную собственность) 15.1.2
internal organization (внутренняя организация) 6.1
internal processing, control of (внутренняя обработка, управление) 12.2.2
inventory of assets (инвентаризация активов) 7.1.1
isolation of sensitive systems (изоляция чувствительных систем) 11.6.2

K

key management (управление ключами) 12.3.2

L

labeling and handling of information (маркировка и обработка информации) 7.2.2
leakage of information (утечка информации) 12.5.4
learning from information security incidents (извлечение уроков из инцидентов информационной безопасности) 13.2.2
legal requirements, compliance with (соответствие требованиям законодательства) 15.1
legislation, identification of applicable (законодательство, определение применимости) 15.1.1
limitation of connection time (ограничения времени соединения) 11.5.6
loading area (зоны отгрузки) 9.1.6
logs (журналы регистрации)
— administrator and operator logs (журналы регистрации администратора и оператора) 10.10.4
— audit logging (контрольная регистрация) 10.10.1
— fault logging (регистрация неисправностей) 10.10.5
— protection of log information (защита информации журналов регистрации) 10.10.3
log-on procedures (процедуры начала сеанса) 11.5.1

M

maintenance (техническое обслуживание)
— and acquisition and development of information systems (и приобретение и эксплуатация информационных систем) 12
— of equipment (оборудования) 9.2.4
malicious code (вредоносная программа)
— controls against (меры и средств контроля и управления против) 10.4.1
— protection against (защита от) 10.4
management (менеджмент/управление)
— of assets (активов) 7
— of business continuity (непрерывности бизнеса) 14
— of capacity (производительностью) 10.3.1
— of changes (изменениями) 10.1.2
— of changes to third party services (изменениями услуг третьей стороны) 10.2.3
— commitment to information security (обязательства по отношению к) 6.1.1
— of communications and operations (коммуникаций и работ) 10
— of cryptographic keys (криптографическими ключами) 12.3.2
— of information security aspects of business continuity (аспекты информационной безопасности в рамках непрерывности бизнеса) 14.1
— of information security incidents (инцидентов информационной безопасности) 13, 13.2
— of network security (безопасности сети) 10.6
— of privileges (привилегиями) 11.2.2
— of removable computer media (сменных носителей информации) 10.7.1
— responsibilities (обязанности) 8.2.1
— system for passwords (система для паролей) 11.5.3
— of technical vulnerabilities (технических уязвимостей) 12.6
— of user access (доступа пользователей) 11.2
— of user passwords (паролями пользователей) 11.2.3
media (носители информации)
— disposal of (утилизация) 10.7.2
— handling (обращение с) 10.7
— in transit (при транспортировке) 10.8.3
— removable (сменные) 10.7.1
message integrity (целостность сообщений) 12.2.3
messaging electronic (электронные сообщения) 10.8.4
misuse of information processing facilities, prevention of (нецелевое использование средств обработки информации, предотвращение) 15.1.5
mobile code (мобильная программа)
— controls against (меры и средства контроля и управления против) 10.4.2
— protection against (защита от) 10.4
mobile computing (мобильная вычислительная техника) 11.7
— mobile computing and communications (мобильная вычислительная техника и связь) 11.7.1
monitoring (мониторинг) 10.10
— and review, of third party services (и анализ услуг третьей стороны) 10.2.2
— system use (использование системы) 10.10.2

N

network (сеть)
— access control of (управление доступом к) 11.4
— connection control of (управление сетевыми соединениями) 11.4.6
— controls (меры и средства контроля и управления) 10.6.1
— equipment identification in (идентификация оборудования в) 11.4.3
— routing control of (управление маршрутизацией) 11.4.7
— security, management of (менеджмент безопасности) 10.6
— segregation in (разделение в) 11.4.5
— services, policy on their use (услуги, политика их использования) 11.4.1
— services, security of (услуги, безопасность) 10.6.2
non-repudiation (неотказуемость) 2.5
— services (услуги) 12.3.1

O

offices, rooms and facilities, securing (здания, производственные помещения и оборудование, безопасность) 9.1.3
on-line transactions (транзакции в режиме онлайн) 10.9.2
operating (эксплуатируемый)
— procedures, documented (процедуры, документальное оформление) 10.1.1
— system access control (управление доступом к системе) 11.5
— system changes, technical review of (изменения системы, техническая проверка) 12.5.2
operational (эксплуатационный)
— procedures and responsibilities (процедуры и обязанности) 10.1
— software, control of (программное обеспечение, управление) 12.4.1
operations and communications management (менеджмент коммуникаций и работ) 10
operator logs (журнал регистрации оператора) 10.10.4
organizational records, protection of (документы организации, защита) 15.1.3
other information (дополнительная информация) 3.2
output data validation (подтверждение выходных данных) 12.2.4
outsourced software development (аутсорсинг разработки программного обеспечения) 12.5.5
ownership of assets (владение активами) 7.1.2

P

passwords (пароли)
— management of, user (управление, пользователь) 11.2.3
— management system for (система управления) 11.5.3
— use of (использование) 11.3.1
personal information, privacy of (персональные данные, защита) 15.1.4
physical (физическая)
— and environmental security (и защита от воздействий окружающей среды) 9
— entry controls (меры и средства контроля и управления физическим входом) 9.1.2
— media in transit (физические носители информации при транспортировке) 10.8.3
— security perimeter (периметр зоны безопасности) 9.1.1
plans for business continuity (планы обеспечения непрерывности бизнеса)
— developing and implementing them (их разработка и внедрение) 14.1.3
— testing, maintaining and re-assessing them (их тестирование, поддержка и пересмотр) 14.1.5
policy (политика) 2.8
— on access control (по управлению доступом) 11.1
— on clear desk and clear screen («чистого стола» и «чистого экрана») 11.3.3
— on information exchange (обмена информацией) 10.8.1
— on information security (информационной безопасности) 5.1
— on the use of cryptographic controls (использования криптографических мер и средств контроля и управления) 12.3.1
— on use of network services (использования сетевых услуг) 11.4.1
— security (безопасности) 5
prevention of misuse of information processing facilities (предотвращение нецелевого использования средств обработки информации) 15.1.5
prior to employment (перед трудоустройством) 8.1
privilege management (управление привилегиями) 11.2.2
procedures (процедуры)
— on change control (управления изменениями) 12.5.1
— on information exchange (обмена информацией) 10.8.1
— for information handling (обработки информации) 10.7.3
— for log-on (начало сеанса) 11.5.3
— operational (эксплуатационные) 10.1, 10.1.1
— and responsibilities for incident management (обязанности по менеджменту инцидентов) 13.2.1
program source code, access control to (исходный текст программ, управление доступом к) 12.4.3
property, removal of (имущество, перемещение) 9.2.7
property rights, intellectual (права на собственность, интеллектуальная) 15.1.2
protection (защита)
— against malicious and mobile code (от вредоносной и мобильной программы) 10.4
— of information system audit tools (инструментальные средства аудита информационных систем) 15.3.2
— of log information (информации журналов регистрации) 10.10.3
— of organizational records (документы организации) 14.1.3
— of system test data (тестовые данные системы) 12.4.2

public access, delivery and loading area (зоны общего доступа, приемки и отгрузки) 9.1.6
publicly available information (общедоступная информация) 10.9.3

R

regulation of cryptographic controls (регулирование криптографических мер и средств контроля и управления) 15.1.6
reliability (надежность) 2.5
remote diagnostic and configuration port protection (защита портов дистанционной диагностики и конфигурации) 11.4.4
removable media, management of (сменные носители информации, менеджмент) 10.7.1
removal (аннулирование/перемещение)
— of access rights (прав доступа) 8.3.3
— of property (имущества) 9.2.7
reporting (оповещение)
— information security events (о событиях информационной безопасности) 13.1, 13.1.1
— security weaknesses (уязвимости информационной безопасности) 13.1, 13.1.2
responsibilities (обязанности)
— allocation of information security (распределение по обеспечению информационной безопасности) 6.1.3
— and roles (и роли)8.1.1
— for termination (прекращение) 8.3.1
— of management (руководства) 8.2.1
— operational (эксплуатационные) 10.1
— and procedures for incident management (и процедуры по менеджменту инцидентов) 13.2.1
— user (пользователь) 11.3
restrictions of changes to software packages (ограничения на изменения пакетов программ) 12.5.3
return of assets (возврат активов) 8.3.2
re-use of equipment (повторное использование оборудования) 9.2.6
review (проверка/пересмотр)
— of information security (информационной безопасности) 6.1.8
— of information security policy (политики информационной безопасности) 5.1.2
— and monitoring, of third party services (и мониторинг, услуги третьей стороны) 10.2.2
— of user access rights (права доступа пользователей) 11.2.4
risk (риск) 2.9
— analysis (анализ) 2.10
— assessment (оценка) 2.11, 4.1
— assessment and business continuity (непрерывность бизнеса и оценка риска) 14.1.2
— evaluation (оценивание) 2.12
— management (менеджмент) 2.13
— treatment (обработка) 2.14, 4.2
risks related to external parties (риски, являющиеся следствием работы со сторонними организациями) 6.2.1
roles and responsibilities (роли и обязанности) 8.1.1
rooms, offices and facilities, securing (производственные помещения, здания и оборудование) 9.1.3
routing control in networks (управление сетевой маршрутизацией) 11.4.7

S

screening (предварительная проверка) 8.1.2
secure areas (зоны безопасности) 9.1
— working in (работа в) 9.1.5
securing offices, rooms and facilities (безопасность зданий, производственных помещений и оборудования) 9.1.3
security (безопасность)
— in development and support processes (в процессах разработки и поддержки) 12.5
— of human resources (связанная с персоналом) 8
— of equipment (оборудования) 9.2
— of equipment off-premises (оборудования вне помещений организации) 9.2.5
— of network services (сетевых услуг) 10.6.2
— policy (политика) 5
— policy, compliance with (политика, соответствие) 15.2.1
— requirements analysis and specification (анализ требований безопасности и спецификация) 12.1.1
— of system documentation (системная документация) 10.7.4
— of system files (системные файлы) 12.4
— weaknesses, reporting of (уязвимости, оповещение о) 13.1.2
segregation of duties (разделение обязанностей) 10.1.3

— in networks (в сетях) 11.4.5
sensitive system isolation (изоляция чувствительных систем) 11.6.2
separation of development, test and operational facilities (разделение средств разработки, тестирования и эксплуатации) 10.1.4
service delivery (предоставление услуг) 10.2.1
— management, of third parties (менеджмент, третьей стороны) 10.2
services, for electronic commerce (услуги, электронная торговля) 10.9
session time-out (лимит времени сеанса связи) 11.5.5
siting of equipment (размещение оборудования) 9.2.1
software (программное обеспечение)
— development, outsourced (разработка, аутсорсинг) 12.5.5
— operational, control of (эксплуатируемое, управление) 12.4.1
— packages, restrictions on changes (пакеты программ, ограничение на изменение) 12.5.3
source code, access control to (исходный текст программ, управление доступом к) 12.4.3
standards and security policies, compliance with (стандарты и политики безопасности, соответствие) 15.2, 15.2.1
support and development processes, security in (процессы разработки и поддержки, безопасность в) 12.5
system (система)
— acceptance (приемка) 10.3.2
— acquisition, development and maintenance (приобретение, разработка и эксплуатация) 12
— audit considerations (рассмотрения аудита) 15.3
— audit controls (меры и средства контроля и управления аудита) 15.3.1
— audit tools, protection of (инструментальные средства аудита, защита) 15.3.2
— documentation, security of (документация, безопасность) 10.7.4
— files, security of (файлы, безопасность) 12.4
— planning and acceptance (планирование и приемка) 10.3
— sensitive, isolation of (чувствительность, изоляция) 11.6.2
— test data, protection of (тестовые данные, защита) 12.4.2
— use, monitoring of (использование, мониторинг) 10.10.2
— utilities, use of (утилиты, использование) 11.5.4

T

technical (технический)
— compliance checking (проверка соответствия) 15.2.2
— review of applications after operating system changes (проверка прикладных программ после изменений эксплуатируемой системы) 12.5.2
— vulnerabilities, control of (уязвимости, управление) 12.6.1
— vulnerability management (менеджмент уязвимостей) 12.6
teleworking (дистанционная работа) 11.7, 11.7.2
termination of employment (прекращение занятости) 8.3
termination responsibilities (прекращение обязанностей) 8.3.1
terms and conditions of employment (условия занятости) 8.1.3
test (тест)
— data, protection of (данные, защита) 12.4.2
— and development and operational facilities, separation of (средства разработки, тестирования и эксплуатации, разделение) 10.1.4
— testing, maintaining and re-assessing business continuity plans (тестирование, поддержка и пересмотр планов непрерывности бизнеса) 14.1.5
third party (третья сторона) 2.15
— addressing security in agreements (рассмотрение требований безопасности в договорах) 6.2.3
— service delivery management (менеджмент оказания услуг) 10.2
— services, managing changes to (управление изменениями услуг) 10.2.3
— services, monitoring and review (мониторинг и анализ услуг) 10.2.2
threat (угроза) 2.16
training, awareness and education in information security (тренинг, обучение и осведомленность в области информационной безопасности) 8.2.2
transactions, on-line (транзакции, режим онлайн) 10.9.2

U

unattended user equipment (оборудование пользователя, оставленное без присмотра) 11.3.2
user (пользователь)
— access management (менеджмент доступа) 11.2
— access rights, review of (права доступа, пересмотр) 11.2.4

— authentication for external connections (аутентификация для внешних соединений) 11.4.2
— identification and authentication (идентификация и аутентификация) 11.5.2
— password management (управление паролями) 11.2.3
— registration (регистрация) 11.2.1
— responsibilities (обязанности) 11.3
— unattended user equipment (оборудование пользователя, оставленное без присмотра) 11.3.2
utilities (утилиты/поддерживающие услуги)
— supporting (поддерживающие) 9.2.2
— system (системные) 11.5.4

V

validation (подтверждение)
— of input data (входных данных) 12.2.1
— of output data (выходных данных) 12.2.4
virus protection (защита от вирусов) 11.7.1, 11.7.2
vulnerability (уязвимость) 2.17
— control of technical vulnerabilities (управление техническими уязвимостями) 12.6.1
— technical vulnerability management (менеджмент технических уязвимостей) 12.6

W

working in secure areas (работа в зонах безопасности) 9.1.5

УДК 001.4:025.4:006.354 ОКС 35.040 Т00

Ключевые слова: информационная безопасность, мера и средство контроля и управления, физическая безопасность, менеджмент информационной безопасности, менеджмент инцидентов, менеджмент непрерывности бизнеса, менеджмент активов, риск, зона безопасности, управление доступом, инцидент

Редактор *В. Л. Савинова*
Технический редактор *В. Н. Прусакова*
Корректор *Л. Я. Митрофанова*
Компьютерная верстка *Т. Ф. Кузнецовой*

Сдано в набор 20.06.2014. Подписано в печать 20.08.2014. Формат $60\times84^{1}/_{8}$. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 12,09. Уч.-изд. л. 11,00. Тираж 62 экз. Зак. 1057

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

gost.e-ecolog.ru