ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационные технологии

СРЕДСТВА ОБЕСПЕЧЕНИЯ

Свод правил по управлению защитой информации

СТ РК ИСО/МЭК 27002-2009
(ISO/IEC 27002:2005, IDT)

Издание официальное

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

Астана

Предисловие

1 ПОДГОТОВЛЕН И ВНЕСЕН Республиканским государственным предприятием "Казахстанский институт стандартизации и сертификации" Комитета по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан и Техническим комитетом по стандартизации № 61 «Автоматическая идентификация»

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Председателя Комитета по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан от 17 ноября 2009 года № 564-од

3 Настоящий стандарт идентичен международному стандарту ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management (Информационные технологии. Средства обеспечения. Свод правил по управлению защитой информации)

Перевод с английского языка (en)

Степень соответствия – идентичная (IDT)

4 СРОК ПЕРВОЙ ПРОВЕРКИ **2014 год**
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ **5 лет**

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в указателе «Нормативные документы по стандартизации», а текст изменений – в ежемесячных информационных указателях «Государственные стандарты». В случае пересмотра (отмены) или замены настоящего стандарта соответствующая информация будет опубликована в информационном указателе «Государственные стандарты»

Содержание

Введение

1 Что такое информационная безопасность?

Информация - это актив, который, подобно другим активам организации, имеет ценность и, следовательно, должен быть защищен надлежащим образом. Информационная безопасность защищает информацию от широкого диапазона угроз с целью обеспечения уверенности в непрерывности бизнеса, минимизации ущерба, получения максимальной отдачи от инвестиций, а также реализации потенциальных возможностей бизнеса. В результате этой возрастающей взаимосвязанности, информация на сегодняшний день подвергается растущему числу и широкому кругу опасностей и уязвимостей (см. Рекомендации ОЭСР для Безопасности Информационных Систем и Сетей).

Информация может существовать в различных формах. Она может быть напечатана или написана на бумаге, храниться в электронном виде, передаваться по почте или с использованием электронных средств связи, демонстрироваться на пленке или быть выражена устно. Безотносительно формы выражения информации, средств ее распространения или хранения она должна всегда быть адекватно защищена.

Информационная безопасность достигается путём реализации соответствующего комплекса мероприятий по управлению информационной безопасностью, которые могут быть представлены политиками, методами, процедурами, организационными структурами и функциями программного обеспечения. Эти мероприятия должны быть установлены, внедрены, усовершенствованы там, где это необходимо, и должны обеспечить достижение целей информационной безопасности организации.

2 Необходимость информационной безопасности

Информация, поддерживающие ее процессы, информационные системы и сетевая инфраструктура являются существенными активами организации. Конфиденциальность, целостность и доступность информации могут существенно способствовать обеспечению конкурентоспособности, ликвидности, доходности, соответствия законодательству и деловой репутации организации.

Организации, их информационные системы и сети все чаще сталкиваются с различными угрозами безопасности, такими как компьютерное мошенничество, шпионаж, вредительство, вандализм, пожары или наводнения. Такие источники ущерба, как компьютерные вирусы, компьютерный взлом и атаки типа отказа в обслуживании, становятся более распространенными, более агрессивными и все более изощренными.

Зависимость от информационных систем и услуг означает, что организации становятся все более уязвимыми по отношению к угрозам безопасности. Взаимодействие сетей общего пользования и частных сетей, а также совместное использование информационных ресурсов затрудняет управление доступом к информации. Тенденция к использованию распределенной обработки данных ослабляет эффективность централизованного контроля.

При проектировании многих информационных систем вопросы безопасности не учитывались. Уровень безопасности, который может быть достигнут техническими средствами, имеет ряд ограничений и, следовательно, должен сопровождаться надлежащими организационными мерами. Выбор необходимых мероприятий по управлению информационной безопасностью требует тщательного планирования и внимания к деталям.

Управление информационной безопасностью нуждается, как минимум, в участии всех сотрудников организации. Также может потребоваться участие поставщиков, клиентов или акционеров. Кроме того, могут потребоваться консультации специалистов сторонних организаций.

3 Как определить требования к информационной безопасности

Организация должна определить свои требования к информационной безопасности с учетом следующих трех факторов:

Во-первых, оценка рисков организации. Принимая во внимание всю деловую стратегию и задачи организации, посредством оценки рисков происходит выявление угроз активам организации, оценка уязвимости соответствующих активов и вероятности возникновения угроз, а также оценка возможных последствий.

Во-вторых, юридические, законодательные, регулирующие и договорные требования, которым должны удовлетворять организация, её торговые партнёры, подрядчики, и поставщики услуг, и их социально-культурное окружение.

В-третьих, специфический набор принципов, целей и требований, разработанных организацией в отношении обработки информации.

4 Оценка рисков информационной безопасности

Требования к информационной безопасности определяются с помощью систематической оценки рисков. Решения о расходах на мероприятие по управлению информационной безопасностью должны приниматься, исходя из возможного ущерба, нанесенного бизнесу в результате нарушения информационной безопасности.

Результаты этой оценки помогут в определении конкретных мер и приоритетов в области управления рисками, связанными с информационной безопасностью, а также внедрению мероприятий по управлению информационной безопасностью с целью минимизации этих рисков.

Оценку рисков следует периодически повторять для адресации изменений, которые могут влиять на результаты оценки рисков.

Оценка степени риска должна быть повторена периодически, чтобы обратиться к любым изменениям, которые могли бы влиять на результаты оценки степени риска.

Подробную информацию о рисках безопасности можно найти в Разделе 4.1 «Оценка рисков безопасности».

5 Выбор элементов контроля управления информационной безопасностью

После того, как определены требования к информационной безопасности, следует выбрать и внедрить такие мероприятия по управлению информационной безопасностью, которые обеспечат снижение рисков до приемлемого уровня. Эти мероприятия могут быть выбраны из настоящего стандарта, других источников, а также могут быть разработаны собственные мероприятия по управлению информационной безопасностью, удовлетворяющие специфическим потребностям организации.

Выбор мероприятий безопасности зависит от организационных решений, основанных на критерии допустимого риска, опций обработки рисков, и общего подхода к управлению рисками, применённого к данной организации, подлежащего государственным и международным нормам и законодательству.

Некоторые мероприятия по управлению информационной безопасностью, приведенных в настоящем стандарте, могут рассматриваться как руководящие принципы для управления информационной безопасностью и применяться для большинства организаций. Более подробно такие мероприятия рассматриваются ниже, в разделе «Отправная точка для внедрения информационной безопасности».

Более подробная информация о выборе мероприятий и других опциях обработки рисков содержится в разделе 4.2 «Обработка рисков безопасности».

6 Отправная точка для внедрения информационной безопасности

Отдельные мероприятия по управлению информационной безопасностью могут рассматриваться как руководящие принципы для управления информационной безопасностью и служить оптимальный исходный пункт для ее внедрения. Такие мероприятия либо основываются на ключевых требованиях законодательства, либо рассматриваются как общепринятая практика в области информационной безопасности.

Ключевыми мерами контроля с точки зрения законодательства являются:

a) обеспечение конфиденциальности персональных данных (15.1.4);

b) защита учетных данных организации (15.1.3);

c) права на интеллектуальную собственность (15.1.2).

Мероприятия по управлению информационной безопасностью, рассматриваемые как общепринятая практика в области информационной безопасности, включают:

a) наличие документа, описывающий политику информационной безопасности (5.1.1);

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

c) обучение вопросам информационной безопасности (8.2.2);

d) правильную обработку в приложениях (12.2);

e) управление технической уязвимостью (12.6);

f) управление непрерывностью бизнеса (14);

g) информирование об инцидентах, связанных с информационной безопасностью (13.2).

Перечисленные мероприятия применимы для большинства организаций и информационных сред.

Следует отметить, что, все приведенные в настоящем стандарте мероприятия являются важными, уместность какой-либо меры должна определяться в свете конкретных рисков, с которыми сталкивается организация. Следовательно, несмотря на то, что вышеописанный подход рассматривается как отправная точка для внедрения мероприятий по обеспечению информационной безопасности, он не заменяет выбор мероприятий по управлению информационной безопасностью, основанный на оценке рисков.

7 Важнейшие факторы успеха

Практика показывает, что для успешного внедрения информационной безопасности в организации являются следующие факторы:

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

b) согласованность подхода к внедрению информационной безопасности с корпоративной культурой;

c) видимая поддержка и заинтересованность со стороны руководства;

d) четкое понимание требований безопасности, оценка рисков и управление рисками;

e) обеспечение понимания необходимости применения мер информационной безопасности руководством и сотрудниками организации;

f) передача инструкций в отношении политики информационной безопасности и соответствующих стандартов всем сотрудникам и контрагентам;

g) обеспечение финансирования деятельности по управлению информационной безопасностью;

h) обеспечение необходимого обучения и подготовки;

i) установление эффективного процесса управления инцидентами, относящимися к информационной безопасности;

установление эффективного информационного процесса контроля происшествий безопасности;

j) всесторонняя и сбалансированная система измеряемых показателей, используемых для оценки эффективности управления информационной безопасностью и предложений по ее улучшению.

8 Разработка собственных руководств организации

Настоящий стандарт должен расцениваться как отправная точка для разработки руководства под конкретные нужды организации. Не все инструкции и мероприятия, приведенные в настоящем стандарте, могут быть применимы.

Более того, могут потребоваться дополнительные меры, не включенные в настоящий стандарт. В этом случае может быть полезным сохранение перекрестных ссылок, которые облегчат проверку соответствия, проводимую аудиторами и партнерами по бизнесу.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационные технологии

СРЕДСТВА ОБЕСПЕЧЕНИЯ

Свод правил по управлению защитой информации

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

Дата введения 2010-07-01

1 Область применения

Настоящий стандарт устанавливает свод правил по управлению информационной безопасностью лицам, ответственным за планирование, реализацию или поддержку решений безопасности в организации. Указанные в настоящем стандарте задачи задают направление для достижения общепринятых целей управления информационной безопасностью.

Задачи и элементы управления настоящего стандарта предназначены для внедрения с целью соответствия определенным требованиям, выявленным при оценке риска. Настоящий стандарт предназначен для обеспечения общих основ для разработки стандартов безопасности и выбора практических мероприятий по управлению безопасностью в организации, а также в интересах обеспечения доверия в деловых отношениях между организациями.

2 Нормативные ссылки

Для применения настоящего стандарта необходимы следующие ссылочные нормативные документы:

СТ РК 1.9-2007 Государственная система технического регулирования Республики Казахстан. Порядок применения международных, региональных и национальных стандартов иностранных государств, других нормативных документов по стандартизации в Республике Казахстан.

СТ РК ИСО 10007:2007 Системы менеджмента качества. Менеджмент конфигурации. Основные требования.

СТ РК ИСО/МЭК 11770-1-2008 Информационные технологии. Методы и средства обеспечения безопасности. Управление ключами. Часть 1. Основные положения.

СТ РК ИСО/МЭК 13335-1-2008 Информационные технологии. Методы и средства обеспечения безопасности. Управление защитой информационных технологий. Часть 1. Общие понятия и модели для управления защитой информационных и коммуникационных технологий.

СТ РК ИСО/МЭК ТО 13335-3-2008 Информационные технологии. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий. Часть 3. Методические указания по управлению защитой информационных технологий.

Издание официальное

СТ РК ИСО/МЭК 15408-1-2006 Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

СТ РК ИСО 15489-1:2001 Информация и документация. Оперативный учет. Часть 1. Общие положения.

СТ РК ИСО/МЭК 18028-4-2007 Информационные технологии. Методы обеспечения защиты. Защита сети информационных технологий. Часть 4. Защита удаленного доступа.

СТ РК ИСО 19011:2002 Рекомендации по аудиту систем менеджмента качества и/или охраны окружающей среды.

ИСО/МЭК Руководство 2:1996 Стандартизация и смежные виды деятельности. Общий словарь.*

ИСО/МЭК Руководство 73:2002 Управление риском. Словарь. Руководящие указания по использованию в стандартах.*

ИСО/МЭК 9796-2:2002 Информационные технологии. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 2. Механизмы на основе целочисленной факторизации.*

ИСО/МЭК 9796-3:2006 Информационные технологии. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 3. Механизмы на основе дискретного логарифма.*

ИСО/МЭК 12207:2008 Информационные технологии. Процессы жизненного цикла программного обеспечения.*

ИСО/МЭК 14888-1:2008 Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 1. Общие положения.*

ИСО/МЭК ТО 18044:2004 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.*

ПРИМЕЧАНИЕ При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов и классификаторов по ежегодно издаваемому информационному указателю «Нормативные документы по стандартизации» по состоянию на текущий год и соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) документом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения, структура и разделы настоящего стандарта, основные категории безопасности

3.1 Термины и определения

В настоящем стандарте применяются следующие термины с соответствующими определениями:

3.1.1 **Активы** (asset): Все, что имеет ценность для организации в соответствии с СТ РК ИСО/МЭК 13335-1.

3.1.2 **Контроль** (control): Средства управления рисками, включая политику, процедуры, рекомендации, инструкции или организационные структуры, которые могут иметь административный, технический, управленческий или правовой характер.

ПРИМЕЧАНИЕ Термин «контроль» также используется как синоним меры предосторожности или противодействия.

* Применяется в соответствии с СТ РК 1.9.

3.1.3 **Рекомендации** (guideline): Описание, поясняющее действия и способы их выполнения, необходимые для достижения установленных целей, в соответствии с СТРК ИСО/МЭК 13335-1.

3.1.4 **Средство(а) обработки информации** (information processing facilities): Любая система обработки информации, сервис или инфраструктура, или их физические места размещения.

3.1.5 **Информационная безопасность** (information security): Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, не отказуемости, подотчетности, аутентичности и достоверности информации или средства ее обработки.

3.1.6 **Событие информационной безопасности** (information security event): Идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью в соответствии с ИСО/МЭК ТО 18044.

3.1.7 **Инцидент информационной безопасности** (information security incident): Любое непредвиденное или не желательное событие, которое может нарушить деятельность или информационную безопасность, в соответствии с ИСО/МЭК 18044.

3.1.8 **Политика** (policy): Общие намерения и направления, официально объявленные руководством.

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

ПРИМЕЧАНИЕ Определение на сочетание вероятности события и его последствий (см. Руководство ИСО/МЭК 73).

3.1.10 **Анализ риска** (risk analysis): Систематический процесс определения величины риска в соответствии с Руководством ИСО/МЭК 73.

3.1.11 **Оценка рисков** (risk assessment): Процесс, объединяющий идентификацию риска, анализ риска и оценивание риска в соответствии с Руководством ИСО/МЭК 73.

3.1.12 **Оценивание риска** (risk evaluation): Процесс сравнения количественно оцененного риска с заданными критериями риска для определения его значимости в соответствии с Руководством ИСО/МЭК 73.

3.1.13 **Управление рисками** (risk management): Скоординированные действия по руководству и управлению организацией в отношении риска.

ПРИМЕЧАНИЕ Управление рисками включает в себе оценку рисков, обработку рисков, принятие рисков и систему рисков (см. Руководство ИСО/МЭК 73).

3.1.14 **Обработка рисков** (risk treatment): Процесс выбора и осуществления мер по модификации рисков (см. Руководство ИСО/МЭК 73).

3.1.15 **Третья сторона** (third party): Лицо или организация, признанная как независимая сторона в отношении рассматриваемого вопроса (см. Руководство ИСО/МЭК 2).

3.1.16 **Угроза** (threat): Потенциальная причина инцидента, который может нанести ущерб системе или организации в соответствии с СТ РК ИСО/МЭК 13335-1.

3.1.17 **Уязвимость** (vulnerability): Слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами в соответствии с СТ РК ИСО/МЭК 13335-1.

3.2 Структура настоящего стандарта

Настоящий стандарт содержит 11 разделов по управлению информационной безопасности, содержащих в общей сложности 39 основных категорий безопасности и один вводный раздел, представляющий оценку и обработку рисков.

3.3 Разделы

Каждый раздел содержит в себе несколько основных категорий безопасности. Ниже приведены наименования одиннадцати разделов (в каждый раздел из которых включены несколько основных категорий безопасности):

a) Политика информационной безопасности (1);
b) Организация информационной безопасности (2);
c) Управление активами (2);
d) Безопасность персонала (3);
e) Физическая безопасность и безопасность окружающей среды (2);
f) Управление коммуникациями и операциями (10);
g) Управление доступом (7);
h) Приобретение, разработка и поддержка информационных систем (6);
i) Управление инцидентами информационной безопасности (2);
j) Управление непрерывностью бизнеса (1);
k) Соответствие требованиям (3).

ПРИМЕЧАНИЕ Порядок расположения разделов в настоящем стандарте не зависит от их важности. В зависимости от обстоятельств, все разделы могут быть важны, следовательно, каждая организация, применяющая настоящий стандарт, должна идентифицировать используемые разделы, их важность и применение в индивидуальных процессах деловой активности. Кроме того, списки в настоящем стандарте не упорядочены по приоритетам, за исключением случаев, когда дается иное в примечании.

3.4 Основные категории безопасности

Каждая основная категория безопасности содержит:

a) задачу управления, указывающую на то, что должно быть достигнуто; и

b) один или несколько элементов управления, которые могут применяться для решения задачи управления.

Характеристики управления систематизируются следующим образом:

Контроль

Определяет специальный управляющий оператор для выполнения цели управления.

Руководство по внедрению

Предоставляет более подробную информацию о внедрении управления и решения задач управления. Некоторые руководства не могут использоваться во всех случаях, следовательно, более подходящими могут оказаться другие пути внедрения управления.

Прочая информация

Обеспечивает дальнейшую информацию, которую необходимо учитывать в определенных случаях, например: правовые вопросы и ссылки на другие стандарты.

4 Оценка и обработка рисков

4.1 Оценка рисков безопасности

Оценка рисков должна идентифицировать, определять количество и располагать в порядке очередности риски согласно критериям допустимости риска и задач, актуальных для данной организации. Результаты должны направлять и определять надлежащие действия руководства и приоритеты для управления рисками информационной безопасности, а также для внедрения элементов управления, отобранных для зашиты этих

рисков. Процесс оценки рисков и отбора элементов управления может потребовать многократного выполнения с целью охвата различных частей организации или отдельных информационных систем.

Оценка рисков должна включать в себя систематический подход к оценке величины рисков (анализ рисков) и процесс сравнения рассчитанных рисков согласно критериям рисков в целях определения значимости рисков (оценка рисков).

Оценка рисков должна проводиться на регулярной основе для своевременного реагирования на изменения рисков и требований по безопасности и, например: изменения активов, угроз, степени защищенности, воздействия, оценки рисков, а также при значительных изменениях. Эти оценки рисков должны иметь систематический характер для получения сопоставимых и воспроизводимых результатов.

Для того чтобы быть эффективной, оценка рисков информационной безопасности должна иметь четко определенную область охвата по возможности соотноситься с оценкой рисков в других областях.

Область охвата оценки рисков может относиться либо ко всей организации, либо к отдельным частям организации, конкретным информационным системам, либо к особым компонентам или службам системы, где это практически выполнимо, реально и полезно. Примеры методов оценки рисков рассмотрены в СТ РК ИСО/МЭК ТО 13335-3 (Руководство по управлению безопасностью информационных технологий: методы управления за безопасностью информационных технологий).

4.2 Обработка рисков безопасности

Прежде, чем приступить к обработке рисков, организация должна установить критерии допустимости или недопустимости рисков. Риски могут быть допустимыми в тех случаях, когда риск оценен как низкий или стоимость обработки не рентабельна для этой организации. Такие решения оформляются документально.

По каждому риску, идентифицированному в результате оценки рисков, необходимо принимать решение о его обработке. Возможные варианты обработки рисков включают:

a) применение соответствующих элементов управления по уменьшению рисков;

b) сознательное и объективное допущение рисков, при условии, что они четко соответствуют организационной политике к критериям допустимых рисков;

c) избежание рисков путем недопущения действий, которые могут привести к возникновению рисков;

d) передача объединенных рисков другим сторонам, например, страховым компаниям или поставщикам.

Для рисков, при оценке которых было принято решение о применении соответствующих элементов управления, эти элементы отбираются и внедряются для соответствия требованиям, идентифицированным в ходе оценки риска. Элементы управления должны обеспечивать уменьшение рисков до приемлемого уровня с учетом:

a) требований и ограничений государственных и международных законодательств и нормативных правовых актов;

b) задач организации;

c) производственных требований и ограничений;

d) стоимость внедрения и эксплуатации в отношении сниженных рисков,

оставшихся пропорциональными требованиям и ограничениям, принятым в организации;

e) необходимость в поддержании баланса инвестиций во внедрение и применение

элементов управления для предотвращения возможного вреда от нарушения безопасности.

Элементы управления могут выбираться из настоящего стандарта или других групп элементов управления, кроме того, в зависимости от специфичных нужд отдельной организации могут быть разработаны новые элементы управления. Необходимо отметить, что некоторые элементы управления не могут быть приемлемыми для каждой информационной системы или среды, и не могут быть практически осуществимыми для всех организаций. Например, в Разделе 10.1.3 рассмотрена возможность разграничения заданий для предотвращения мошенничества и ошибок. Для небольших организаций разграничение всех заданий может оказаться невозможным, и в таком случае будут необходимы другие пути для решения этой задачи управления. В качестве еще одного примера, в Разделе 10.10 рассматриваются возможности для слежения за использованием системы и сбора данных. Описанные элементы управления, например, регистрация событий, могут вступить в конфликт с применяемым законодательством, например, в части охраны прав личности для клиентов или на рабочем месте.

Элементы контроля информационной безопасности следует учитывать при определении требований к системам и проектам на этапе проектирования. Несоблюдение этого условия может привести к дополнительным затратам и менее эффективным решениям, в худшем случае, к невозможности достижения адекватной безопасности.

Следует помнить, что ни один набор элементов контроля не позволяет достичь абсолютной безопасности, и что необходимы дополнительные действия со стороны руководства для отслеживания, оценки и повышения результативности и эффективности элементов контроля безопасности в целях решения стоящих перед организацией задач.

5 Политика безопасности

5.1 Политика информационной безопасности

Цель: Обеспечить участие высшего руководства организации в решении вопросов, связанных с обеспечением информационной безопасности в соответствии с целями деятельности организации (бизнеса), законами и нормативными актами.

Руководство организации должно четко сформулировать требования политики, проявить и поддержать требования информационной безопасности путем распространения политики информационной безопасности во всей организации.

5.1.1 Документирование политики информационной безопасности

Контроль

Документ, содержащий описание политики информационной безопасности должен быть утвержден руководством, издан и доведен до сведения всех сотрудников организации, а также сторонних организаций.

Руководство по внедрению

Этот документ должен выражать поддержку руководства организации и определять подход к управлению информационной безопасностью, который будет применяться в организации. Данный документ должен включать следующие сведения:

a) определение информационной безопасности, ее общих целей и сферы действия, а также раскрытия значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации (Раздел «Введение»);

b) изложение целей и принципов информационной безопасности, в соответствии с решаемыми задачами, сформулированных руководством;

c) мероприятия по достижению целей и средства управления, в том числе структуры оценки рисков, а также управления рисками;

d) краткое объяснение наиболее существенных для организации политик безопасности, принципов, правил и требований, например:

1) соответствие законодательным требованиям и договорным обязательствам;

2) требования в отношении обучения вопросам безопасности;

3) управление непрерывностью бизнеса;

4) ответственность за нарушения политики безопасности;

e) определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности;

f) ссылки на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры безопасности для конкретных информационных систем, а также правил безопасности, которым должны следовать пользователи.

Такая политика должна быть доведена до сведения всех сотрудников организации в доступной и понятной форме.

Прочая информация

Политика информационной безопасности может быть частью общей документации. Если политика информационной безопасности распространяется вне организации, то необходимо позаботиться о неразглашении важной информации. Дополнительная информация приведена в СТ РК ИСО/МЭК 13335-1.

5.1.2 Пересмотр политики информационной безопасности

Контроль

Политика информационной безопасности должна быть подвергнута анализу и пересмотру через заданные промежутки времени или при возникновении существенных изменений для обеспечения требованиям соответствия, адекватности и эффективности.

Руководство по внедрению

Необходимо, чтобы в организации назначалось ответственное должностное лицо за политику безопасности и утверждалось руководством, которое отвечало бы за ее реализацию, пересмотр и оценку в соответствии с установленной процедурой. В ходе пересмотра следует оценить возможность улучшения положений политики информационной безопасности и процесса управления информационной безопасностью в соответствии с изменениями условий ведения бизнеса, законодательства, изменениями в организационной структуре или информационной системе организации.

При пересмотре политики информационной безопасности должны учитываться результаты пересмотра принципов управления организацией в целом. Периодические пересмотры должны осуществляться в соответствии с установленным графиком и включать:

a) обратную связь от заинтересованных сторон;

b) результаты независимого аудита (6.1.8);

c) предпринятие необходимых корректирующих и предупреждающих действий (см. 6.1.8 и 15.2.1);

d) результаты предыдущих аудитов принципов управления;

e) процесс исполнения и соблюдения политики информационной безопасности;

f) следует оценить возможность улучшения положений политики

информационной безопасности и процесса управления информационной безопасностью в соответствии с изменениями условий ведения бизнеса, доступности ресурсов, законодательства, изменениями в организационной структуре или информационной системе организации;

g) существенные угрозы и уязвимости информационной системы;

h) отчеты об инцидентах в области информационной безопасности (13.1);

i) рекомендации органов государственной власти (6.1.6).

Вывод из пересмотра принципов управления должны включать в себя любые решения и действия, связанные с:

a) усовершенствованием подхода организации по управлению информационной безопасности и ее процессами;

b) улучшением целей и мероприятий по управлению информационной безопасностью;

c) усовершенствованием в распределении ресурсов и обязанностей.

Необходимо ведение записей пересмотра принципов управления.

Пересмотренная политика информационной безопасности должна быть утверждена руководством организации.

6 Организация информационной безопасности

6.1 Внутренняя организация

Цель: Обеспечение управления информационной безопасностью в организации.

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

Следует создавать соответствующие управляющие советы с участием высшего руководства для утверждения политики информационной безопасности, назначения ответственных лиц в области информационной безопасности, а также осуществления координации внедрения мероприятий по управлению информационной безопасностью в организации.

При необходимости следует предусмотреть наличие специалиста по вопросам информационной безопасности внутри организации, к которому могут обращаться заинтересованные сотрудники. Следует налаживать контакты с внешними специалистами по безопасности для того, чтобы быть в курсе отраслевых тенденций, способов и методов ее оценки, а также с целью адекватного реагирования на инциденты нарушения информационной безопасности. Следует поощрять многопрофильный подход к информационной безопасности.

6.1.1 Обязанности руководства по обеспечению информационной безопасности

Контроль

Руководство организации должно постоянно поддерживать заданный уровень информационной безопасности путем внедрения системы менеджмента, а также путем распределения обязанностей и ответственности персонала за ее обеспечение.

Руководство по внедрению

Руководство организации выполняет следующие функции:

a) обеспечение целей информационной безопасности в соответствии с организационными требованиями и использование их в соответствующих процессах;

b) утверждение и пересмотр политики информационной безопасности;

c) пересмотр эффективности внедрения политики информационной безопасности;

d) обеспечение четкого управления и реальной поддержки со стороны руководства инициатив в области безопасности;

e) выделение необходимых ресурсов для обеспечения информационной безопасности;

f) утверждение распределения основных обязанностей и функций в отношении информационной безопасности в организации;

g) внедрение планов и программ по поддержке обеспечения информационной безопасности;

h) обеспечение согласованности средств управления информационной безопасности в организации (см. 6.1.2).

Руководству необходимо в организации ввести консультации со своими специалистами и специалистами из других организаций, проводить анализ и согласовывать результаты консультаций.

В зависимости от организации, распределения обязанностей определяются руководством или существующим органом управления, как совет директоров.

Прочая информация

Дополнительная информация приведена в СТ РК ИСО/МЭК 13335-1.

6.1.2 Координация вопросов обеспечения информационной безопасности

Контроль

Действия по обеспечению информационной безопасности должны координироваться представителями различных подразделений организации, имеющими соответствующие функции и должностные обязанности.

Руководство по внедрению

Как правило, координация вопросов обеспечения информационной безопасности должна предусматривать сотрудничество между менеджерами, пользователями, администраторами, разработчиками приложений, аудиторами и сотрудниками безопасности, специалистами в области страхования и управления рисками, а также обладать знаниями в правовых вопросах и управлении персоналом. Эта деятельность должна:

a) обеспечить безопасность работы выполняемые в соответствии с политикой информационной безопасности;

b) определить способы обработки несоответствий;

c) согласовать конкретные методики и процедуры информационной безопасности, например, такие как оценка рисков, классификация информации с точки зрения требований безопасности;

d) выявить существенные изменения потенциальных угроз и подверженность информации и средств обработки информации к угрозам;

e) оценить адекватность и координировать внедрение конкретных мероприятий по управлению информационной безопасностью;

f) содействовать образованию сотрудников в области информационной безопасности, обучению и пониманию важности информационной безопасности в рамках всей организации;

g) оценить информацию, полученную в ходе мониторинга и пересмотра инцидентов информационной безопасности, и предпринять соответствующие меры по выявленным инцидентам.

Если в организации нет определенной группы специалистов различной специализации, например, потому что такая группа специалистов не соответствует уровню организации, то действия, описанные выше, должны быть предприняты другим соответствующим органом управления или отдельными руководителями.

6.1.3 Распределение обязанностей по обеспечению информационной безопасности

Контроль

Обязанности персонала по обеспечению информационной безопасности должны быть четко определены.

Руководство по внедрению

Политика информационной безопасности (Раздел 5) должна устанавливать общие принципы и правила распределения функций и обязанностей, связанных с обеспечением информационной безопасности в организации. Политику следует дополнить, где необходимо, более детальными руководствами для конкретных областей, систем или услуг. Кроме этого, должна быть четко определена конкретная ответственность в

отношении отдельных материальных и информационных активов и процессов, связанных с информационной безопасностью, например, таких как планирование непрерывности бизнеса.

Ответственное лицо (администратор) информационных активов может передавать свои полномочия по обеспечению безопасности какому-либо руководителю среднего звена или поставщикам услуг. Тем не менее, администратор остается ответственным за обеспечение безопасности актива и должен быть в состоянии определить, что любые переданные полномочия реализуются должным уровнем.

Следует установить границы ответственности каждого руководителя и выполнять следующие правила:

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

b) необходимо назначать ответственных за каждый актив или процедуру безопасности, и детали этой ответственности должны быть документированы (7.1.2);

c) уровни полномочий (авторизации) должны быть ясно определены и документированы.

ПРИМЕЧАНИЕ Под авторизацией понимается определение доступа пользователя к определенным объемам информации; в более широком смысле – разрешение определенных действий.

Прочая информация

Во многих организациях на руководителя службы информационной безопасности возлагается общая ответственность за разработку и внедрение системы информационной безопасности, а также за оказание содействия в определении мероприятий по управлению информационной безопасностью.

В то же время ответственность за определение подлежащих защите ресурсов и реализацию мероприятий по управлению информационной безопасностью в большинстве случаев возлагается на руководителя среднего звена. Общепринятой практикой является назначение ответственного лица (администратора) для каждого информационного актива, в чьи повседневные обязанности входит обеспечение безопасности данного актива.

6.1.4 Процедура получения разрешения на использование средств обработки информации

Контроль

Необходимо определить процедуры получения разрешения на использование новых средств обработки информации.

Руководство по внедрению

При этом могут осуществляться следующие мероприятия по управлению информационной безопасностью:

a) новые средства должны быть соответствующим образом одобрены со стороны руководства пользователей и администраторов средств управления, авторизующих их цель использования. Одобрение следует также получать от менеджеров, ответственного за поддержание среды безопасности локальной информационной системы, чтобы обеспечить уверенность в том, что соответствующие политики безопасности и требования соблюдены;

b) аппаратные средства и программное обеспечение следует проверять на совместимость с другими компонентами системы;

c) использование личных средств обработки информации, например, ноутбуки, домашние компьютеры или портативные устройства для обработки служебной информации) могут быть причиной новых уязвимостей и, следовательно, необходимые

мероприятия по управлению информационной безопасностью, должны быть оценены и авторизованы.

6.1.5 Соглашения о соблюдении конфиденциальности

Контроль

Руководство организации должно определять условия конфиденциальности или вырабатывать соглашения о неразглашении информации в соответствии с целями защиты информации и регулярно их пересматривать.

Руководство по внедрению

Соглашения о конфиденциальности или соглашения о неразглашении используются для уведомления о том, что информация является конфиденциальной или секретной и осуществляется на основании законодательства. Для определения требований соглашений о конфиденциальности и неразглашении информации следует рассматривать следующие мероприятия:

a) определение защищаемой информации (например, конфиденциальной информации);

b) ожидаемую продолжительность соглашения, включая случаи, когда требуется сохранить конфиденциальность на неопределенный срок;

c) необходимые действия в случае аннулирования соглашения;

d) обязанности и действия подписавших сторон, чтобы избежать утечки информации и применения принципа «need to know» (пользователь получает доступ только к данным, безусловно необходимым ему для выполнения конкретной функции);

e) собственность на информацию, коммерческую тайну и интеллектуальную собственность, так как вышеприведенное относится к защите конфиденциальной информации;

f) разрешение использования конфиденциальной информации, и права подписавшихся сторон на использование информации;

g) право на проведение аудита и мониторинга деятельности, связанной с конфиденциальной информацией;

h) процесс уведомлений и сообщений от несанкционированного разглашения или нарушений конфиденциальной информации;

i) условия для сведений могут быть возвращены или уничтожены при прекращении соглашения; и

j) ожидаемые действия должны быть приняты в случае нарушения этого соглашения.

На основании требований безопасности, принятых в организации, может возникнуть другие меры необходимости в заключении соглашения о конфиденциальности и неразглашении информации.

Соглашения о конфиденциальности и неразглашении информации должны соответствовать всем применяемым нормам законодательства (см. 15.1.1).

Требования к конфиденциальности и неразглашении информации следует периодически пересматривать и, когда происходят изменения, которые влияют на эти требования.

Прочая информация

Соглашения о конфиденциальности и неразглашении информации защищают информацию в организации и ставят в известность подписавшие стороны о том, что они несут ответственность за защиту и использование информации, и ее разглашение должно быть только в установленном порядке.

В организации могут быть использованы различные формы конфиденциальности и неразглашения информации.

6.1.6 Взаимодействие с компетентными органами

Контроль

Руководство организации должно поддерживать взаимодействие с соответствующими компетентными органами.

Руководство по внедрению

Организации должны иметь процедуры, определяющие, когда и с кем должны осуществлять взаимодействие с компетентными органами (например, правоохранительные органы, пожарные службы, контролирующие организации), и как своевременно выявить инциденты нарушения информационной безопасности, если возникает подозрение нарушения закона.

Организациям, подвергшим атакам из сети Интернет, возможно потребуется помощь третьих сторон (например, поставщиков услуг сети Интернет или операторов связи) для принятия соответствующих мер против источника атаки.

Прочая информация

Поддержание таких контактов может быть одним из требований для поддержки информационной безопасности, управления инцидентами (Раздел 13.2) или непрерывности бизнеса и процесса планирования (Раздел 14). Взаимодействие с регулирующими органами, также необходимы для прогнозирования и подготовки к предстоящим изменениям в законодательстве или правилах, которые должны соблюдаться организацией. При взаимодействии с другими уполномоченными органами учитывают коммунальное услуги, аварийно-спасательные службы, охраны здоровья и безопасности, например, пожарные службы (в связи с непрерывностью бизнеса), телекоммуникационные услуги (в связи с маршрутизацией связи и ее пригодностью), услуги водоснабжения (на подключение оборудования с системами охлаждения).

6.1.7 Взаимодействие с ассоциациями и профессиональными группами

Контроль

Руководство организации должно поддерживать соответствующее взаимодействие с профессиональными группами, ассоциациями и участвовать (организовывать) в конференциях (форумах) специалистов в области информационной безопасности.

Руководство по внедрению

Членство в профессиональных группах или участие в конференциях (форумах), следует рассматривать как средство для:

a) совершенствования знаний и навыков и соответствия новейшим требованиям в области информационной безопасности;

b) обеспечения полного понимания обстановки в области информационной безопасности;

c) получения своевременных предупреждений о тревожных сигналах, опасности и исправлений, касающиеся атак и уязвимостей;

d) получения доступа к специалистам за консультацией по вопросам информационной безопасности;

e) обмена информацией о новых технологиях, программных продуктах, угроз или уязвимостей;

f) предоставления адекватного реагирования на инциденты нарушения информационной безопасности (см. 13.2.1).

Прочая информация

Соглашения о совместном использовании информации могут заключаться с целью улучшения сотрудничества и координации в вопросах безопасности. Такие соглашения должны определять требования по защите важной информации.

6.1.8 Независимая проверка (аудит) информационной безопасности

Контроль

Порядок организации и управления информационной безопасностью и ее реализация (например, изменения целей и мер управления, политики, процессов и процедур обеспечения информационной безопасности) должны быть подвергнуты независимой проверке (аудиту) через определенные промежутки времени или при появлении существенных изменений в способах реализации мер безопасности.

Руководство по внедрению

Независимая проверка (аудит) должна быть инициирована руководством. Такая независимая проверка (аудит) необходима для обеспечения постоянной пригодности, адекватности и эффективности подхода организации по управлению информационной безопасностью. Проверка (аудит) должна включать оценку возможностей для улучшения и необходимости изменений в подходе к безопасности, включая политику, цели и меры управления.

Такая проверка (аудит) может быть выполнена внутренним аудитом, независимым менеджером или сторонней организацией, специализирующейся на таких проверках, при этом специалисты, привлекаемые к проверке, должны обладать соответствующими навыками и опытом.

Результаты таких проверок должны быть зафиксированы документально, а учетные записи должны быть сохранены.

Если в результате независимой проверки (аудита) выявляется, что осуществление подхода организации по управлению информационной безопасностью является недостаточным или не соответствует направлению информационной безопасности, определенные в документированной политике информационной безопасности (см. 5.1.1), то руководству необходимо предпринять корректирующие действия.

Прочая информация

Области, подлежащие регулярному пересмотру менеджерами (см. 15.2.1), может также рассматриваться независимой проверкой (аудитом).

В методах пересмотра могут содержать опросы руководства, проверка записей или анализ документирования политики информационной безопасности. В СТ РК ИСО 19011, Рекомендации по аудиту систем менеджмента качества и/или охраны окружающей среды (СТ РК ИСО 19011), также могут быть полезны руководства для проведения независимой проверки (аудита), включая разработку и внедрение программ аудита.

В Разделе 15.3 определены вопросы аудита и меры управления аудитом информационных систем, а также использования инструментальных средств аудита.

6.2 Обеспечение безопасности при наличии доступа сторонних организаций к информационным системам

Цель: Поддерживать безопасность информации и средств обработки информации организации при наличии доступа к ним сторонних организаций в процессах обработки и передачи этой информации.

Безопасность информации организации и средств обработки информации не должна снижаться в результате введения программных продуктов или сервисных обслуживании сторонних организаций.

Доступ к средствам обработки информации организации третьих сторон должен контролироваться.

Там, где есть потребность бизнеса в таком доступе третьей стороны, которые могут потребовать доступ к информации организации и средствам обработки информации, а также в случае приобретения дополнительных программных продуктов или организации сервисного обслуживания средств обработки информации, следует производить оценку

риска, определять последствия для безопасности и устанавливать требования к мероприятиям по управлению информационной безопасностью. Такие мероприятия следует согласовывать и определять в контракте с третьей стороной.

6.2.1 Определение рисков, связанных со сторонними организациями

Контроль

Перед предоставлением доступа сторонним организациям к информации и средствам ее обработки в процессе деятельности организации необходимо определять возможные риски для информации и средств ее обработки и реализовывать соответствующие им меры безопасности.

Руководство по внедрению

Там, где предоставлен доступ сторонней организации к информации и средствам обработки, принадлежащим организации, следует производить оценку рисков, определять последствия для безопасности и устанавливать требования к мероприятиям по управлению информационной безопасностью. При определении рисков, связанных с доступом сторонней организации, следует принимать во внимание следующие мероприятия:

a) необходимость доступа сторонней организации к средствам обработки информации;

b) тип доступа к информации и средствам обработки информации для сторонних организаций, например:

1) физический доступ – к офисным помещениям, компьютерным комнатам, серверным;

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

3) сетевое обеспечение связи между организацией и сетью сторонних организаций, например, постоянное подключение, удаленный доступ;

4) наличие доступа происходит на месте или вне его;

c) значимость и чувствительность вовлеченной информации, и ее критичность для бизнес-операций;

d) меры управления по защите информации, не предназначенные для доступа сторонних организаций;

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

f) как организации, так и персоналу имеющим авторизованный доступ, должен быть четко определен, проверен и подтвержден;

g) различные средства и элементы контроля, используемые сторонней организацией для хранения, обработки, совместного использования и обмена информацией;

h) воздействие доступа, не являющегося доступным для сторонней организации, когда это требуется, или получения сторонней организацией неточной или вводящей в заблуждение информации;

i) действия и процедуры для работы с инцидентами информационной безопасности и потенциальными повреждениями, и условиями пользования для продолжения доступа сторонней организации, в случае инцидента нарушения информационной безопасности;

j) правовых и нормативных требований и других договорных обязательств, имеющих отношение к сторонней организации, которая должна быть принята во внимание;

k) интересы любых других заинтересованных сторон могут быть затронуты в договоренности.

Доступ сторонних организаций к информации организации не должен осуществляться, пока не будут предоставлены и выполнены соответствующие меры

контроля, и по возможности, должно быть подписано соглашение, определяющее условия пользования для подключения или доступа, а также рабочего расположения. Как правило, все требования безопасности и внутренний контроль в результате работы со сторонними организациями, должны быть отражены в соглашениях со сторонними организациями (см. 6.2.2 и 6.2.3).

Необходимо, чтобы сторонняя организация ознакомилась со своими обязанностями, а также принимала на себя ответственность и обязательства, возникающих в результате получения доступа, обработки, совместного использования информации и средств обработки информации, принадлежащих организации.

Прочая информация

Информация может быть под угрозой со стороны сторонних организаций из-за недостаточного управления безопасностью. Меры контроля должны определяться и применяться для управления доступом сторонней организации к средствам обработки информации. Например, если существует специальная потребность в обеспечении конфиденциальности информации, следует заключить соглашение о ее неразглашении.

Организации могут столкнуться с рисками, связанными с межорганизационными процессами, управлением и связью, если применяется высокая степень привлечения, или там, где есть несколько внешних заинтересованных сторон.

Мероприятия по управлению информационной безопасностью, приведенные в Разделах 6.2.2 и 6.2.3, охватывают различные системы сторонней организации, такие как:

a) поставщики услуг, таких как услуг сети Интернет, телефонной связи, организации технического обслуживания и поддержки;

b) управление службы безопасности;

c) покупатели;

d) привлечение внешних средств и/или операций, например систем информационных технологий, службы сбора данных, операции центра телефонного обслуживания;

e) аудиторы и консультанты по вопросам управления и бизнеса;

f) сотрудники, осуществляющие поддержку и сопровождение аппаратных средств и программного обеспечения;

g) сотрудники, осуществляющие уборку, обеспечивающие охрану и другие услуги;

h) студенты и лица, работающие по трудовым соглашениям.

Такие соглашения могут способствовать снижению рисков, связанных со сторонними организациями.

6.2.2 Рассмотрение вопросов безопасности при работе с клиентами

Контроль

Перед предоставлением клиентам права доступа к информации или активам организации необходимо определить и внедрить меры безопасности.

Руководство по внедрению

Необходимо рассматривать следующие условия по решению вопросов безопасности перед предоставлением клиентам права доступа к любым активам организации (в зависимости от вида и степени доступа к данным, и не все из них могут быть применены):

a) защита активов, включая:

1) процедуры по защите активов организации, в том числе информации и программного обеспечения, а также управление известных уязвимостей;

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

3) целостность;

4) ограничения на копирование и раскрытие информации;

b) описание каждого предоставляемого продукта или услуги;

c) различные причины, требования и преимущества для доступа клиентам;

d) соглашения по управлению доступом, охватывающие:

1) разрешенные методы доступа, а также управление и использование уникального идентификатора, типа пользовательских ID и паролей;

2) процесс авторизации в отношении доступа и привилегий пользователей;

3) сведения о том, что любые неавторизованные доступы, запрещены;

4) процесс аннулирования прав доступа или прерывания связи между системами;

e) меры для отчетности, уведомления, а также изучение информации о неточностях (например, личные подробности), инцидентов нарушения информационной безопасности;

f) описание каждой предоставляемой услуги;

g) определение необходимого и неприемлемого обслуживания;

h) право мониторинга и аннулирования любых действий, связанные с активами организации;

i) соответствующие обязательства организации и заказчика;

j) обязательства относительно юридических вопросов, например, законодательства о защите данных с учетом различных национальных законодательств, особенно если контракт относится к сотрудничеству с организациями в других странах (15.1);

k) права интеллектуальной собственности (IPR) и авторские права (15.1.2), а также правовая защита любой совместной работы (6.1.5).

Прочая информация

Требования безопасности, связанные с клиентами, обращающимися к организационным активам, могут измениться значительно в зависимости от средств обработки информации и информации, к которой обращаются. Эти требования безопасности могут быть обращены, используя соглашения клиента, которые содержат все идентифицированные риски и требования безопасности (см. 6.2.1).

В соглашениях со сторонними организациями может быть и участие других сторон.

Соглашения, согласно которым сторонней организации предоставляется доступ к информации, должны содержать разрешение на назначение других правомочных сторон и условий для их доступа и участия.

6.2.3 Рассмотрение требований безопасности в соглашениях со сторонними организациями

Контроль

Соглашения со сторонними организациями должны содержать все требования безопасности, включающие в себя правила доступа к процессам обработки, передачи информации или к управлению информацией или средствами обработки информации организации, а также и в случае приобретения дополнительных программных продуктов или организации сервисного обслуживания средств обработки информации.

Руководство по внедрению

Соглашение (контракт) должно обеспечивать уверенность в том, что нет никакого недопонимания между сторонами.

Для удовлетворения определенных требований безопасности следует учесть следующие положения, включаемые в контракт (см. 6.2.1):

a) общую политику информационной безопасности;

b) защиту активов, включая:

1) процедуры по защите активов организации, в том числе информации и программного обеспечения;

2) любые необходимые способы ограничения физического доступа;

3) мероприятия по управлению информационной безопасностью для обеспечения защиты от вредоносного программного обеспечения (10.4.1);

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

5) мероприятия по обеспечению возвращения или уничтожения информации и активов по окончании соглашения или в установленное время в течение действия контракта;

6) конфиденциальность, целостность и доступность активов (2.1.5);

7) ограничения на копирование и раскрытие информации, предусмотренные в соглашении о конфиденциальности (6.1.5);

c) обучение пользователя и администратора методам и процедурам безопасности;

d) определение процесса информирования о возникающих проблемах в случае непредвиденных обстоятельств;

e) условия для перевода персонала, в случае необходимости;

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

g) четкая структура подотчетности и согласованные форматы предоставления отчётов;

h) четкий и определенный процесс управления изменениями;

i) соглашения по управлению доступом, охватывающие:

1) различные причины, требования и преимущества, необходимые для доступа сторонних лиц;

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

3) процесс авторизации в отношении доступа и привилегий пользователей;

4) требование актуализации списка лиц, имеющих право использовать предоставляемые услуги, а также соответствующего списка прав и привилегий.

5) сведения о всех видах доступа, не авторизованные в четкой форме, являются запрещенными;

6) процесс аннулирования прав доступа или прерывания связи между системами;

j) процедуры отчетности, уведомления и расследования инцидентов нарушения информационной безопасности и выявления слабых звеньев системы безопасности;

k) описание предоставляемого продукта или услуги, а также описание информации, которые должны быть предоставлены вместе с безопасностью классификации (см. 7.2.1);

l) определение необходимого и неприемлемого уровня обслуживания;

m) определение поддающихся проверке критериев эффективности, их мониторинга и отчетности;

n) право мониторинга и аннулирования любых действий, связанные с активами организации;

o) право проводить проверки (аудит) договорных обязанностей или делегировать проведение такого аудита сторонней организации;

p) создание процесса реагирования для решения проблем;

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

r) соответствующие обязательства сторон в рамках контракта;

s) обязательства относительно юридических вопросов например, законодательство о защите данных с учетом различных национальных законодательств, особенно если соглашение относится к сотрудничеству с организациями в других странах (15.1);

t) права интеллектуальной собственности (IPRs) и авторские права (15.1.2), а также правовая защита любой совместной работы (6.1.5);

u) привлечение третьей стороны вместе с субподрядчиками, а также обеспечения их безопасности;

v) условия для пересмотра/прекращения действия соглашения:

1) необходим план непредвиденных ситуаций, если любая из сторон пожелает прекратить отношения по действующему соглашению;

2) следует заключить повторное соглашение, если предусмотрены изменения в требованиях по безопасности;

3) текущую документацию, содержащую списки активов, лицензии, соглашений или прав, относящиеся к ним.

Прочая информация

Соглашения могут существенно отличаться в разных организациях и среди сторонних организаций. Таким образом, необходимо в соглашениях учесть все выявленные риски и требования к безопасности (см. 6.2.1). При необходимости, требуемых мер управления и процедур могут быть подробно изложены в плане обеспечения безопасности.

Для управления информационной безопасностью привлекаются внешние ресурсы, в соглашении указываются способы обеспечения сторонней организацией адекватной безопасности, как это определено оценкой рисков, содержания и адаптации безопасности для выявления и решения с изменениями рисков.

Некоторые различия между привлечением внешних ресурсов и других форм оказания услуг сторонней организации следует включить вопрос об ответственности, планировании переходного периода и потенциальных нарушений работы в течение этого периода, планирование мероприятия и должной осмотрительности, а также сбор и управление информацией о безопасности инцидентов. Таким образом, важно, чтобы организация планировала и управляла переходом к внешним ресурсам и имела подходящие процессы по управлению за изменениями, а также пересмотра/прекращения действия соглашения.

Во избежании задержек по предоставлению услуг со стороны третьих лиц, необходимо предусмотреть в соглашении процедуры длительной обработки.

В соглашениях с третьими лицами может быть и участие других сторон. Соглашения, согласно которым сторонней организации предоставляется доступ к информации, должны содержать разрешение на назначение других правомочных сторон и условий для их доступа и участия.

Прежде всего соглашения должны быть подготовлены самой организацией. При некоторых обстоятельствах, могут возникнуть ситуации, когда соглашение готовят и навязывают организации со стороны третьих сторон. Организация должна обеспечить собственную безопасность и не воздействовать чрезмерным влиянием к требованиям сторонней организации, предусмотренных в этих соглашениях.

7 Управление активами

7.1 Ответственность за защиту активов организации

Цель: Обеспечение соответствующей защиты активов организации.

Все основные информационные активы должны быть учтены и закреплены за ответственными владельцами.

Учет активов помогает обеспечивать уверенность в их надлежащей защите. Необходимо идентифицировать владельцев основных активов и определить их ответственность за поддержание соответствующих мероприятий по управлению информационной безопасностью. Осуществление мероприятий по управлению информационной безопасностью может быть делегировано, но ответственность должна оставаться за назначенным владельцем актива.

7.1.1 Инвентаризация активов

Контроль

Перечень всех важных активов организации должен быть составлен и актуализирован.

Руководство по внедрению

Организация должна быть в состоянии идентифицировать свои активы с учетом их относительной ценности и важности, а также данные о них должны быть документированы. Основываясь на этой информации, организация может обеспечивать заданные уровни защиты, соответствующие ценности и важности активов. Перечень следует составлять и поддерживать для важных активов, связанных с каждой информационной системой. Каждый актив должен быть четко идентифицирован (см.7.1.2) и классифицирован с точки зрения безопасности (см.7.2), его владельцы должны быть авторизованы, а данные о них документированы.

Кроме того, должно быть указано фактическое местоположение актива (это важно в случае восстановления активов при потере или повреждении).ствующие ценности и важности актив Исходя из важности активов, ценности бизнеса и его безопасности, классификация, уровни защиты, соразмерные с важностью активов должны быть определены (более подробная информация об оценке активов и их важности приведена в СТ РК ИСО/МЭК ТО 13335-3).

Прочая информация

Примерами активов, связанных с информационными системами, являются:

a) информационные активы: база данных и файлы данных, системная документация, руководства пользователя, учетные материалы, процедуры эксплуатации или поддержки (обслуживания), планы по обеспечению непрерывности функционирования информационного обеспечения, процедуры действий при сбоях, архивированная информация;

b) активы программного обеспечения: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства разработки и утилиты;

c) физические активы: компьютерное оборудование, оборудование связи, магнитные носители и другое техническое оборудование;

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

e) персонал, квалификация, навыки и опыт;

f) нематериальные активы, такие как престиж (имидж) организации.

Описание активов дает уверенность в том, что обеспечивается эффективная защита активов, и оно может также потребоваться для целей обеспечения безопасности труда, охраны здоровья, страхования или решения финансовых вопросов (управление активами). Процесс составления описи активов - важный аспект управления риском (см. Раздел 4).

7.1.2 Владение активами

Контроль

Вся информация и активы, связанные со средствами обработки информации, должны иметь назначенного во владение[1)] представителя организации.

Руководство по внедрению

Владелец активов несет ответственность за:

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

[1)] Термин «владелец» (owner) лицо или организация, на которую возложена ответственность по контролю за производством, разработкой, поддержке, использованию и безопасности активов. Термин «владелец» не означает, что данное лицо имеет фактические права собственности на этот актив.

b) определение и регулярный пересмотр ограниченного доступа и классификации, принимая во внимание приемлемые политики управления доступом.

Права собственности распространяются на:

a) производственный процесс;

b) определенный вид деятельности;

c) бизнес-приложения; или

d) определенную группу данных.

Прочая информация

Ответственные задания могут быть поручены, например, персоналу, ежедневно работающему с активами, но ответственность за активы несет владелец.

Для сложных информационных систем может быть полезно назначение групп активов, которые действуют совместно, чтобы обеспечить выполнение определенной функции, как «услуги». В этом случае, владелец услуги несет ответственность за доставку услуг, включая функционирование активов, которые обеспечивают ее.

7.1.3 Приемлемое использование активов

Контроль

Правила безопасного использования информации и активов, связанных со средствами обработки информации, должны быть определены, документированы и реализованы.

Руководство по внедрению

Все сотрудники, подрядчики и пользователи сторонних организаций должны соблюдать правила безопасного использования информации и активов, связанных со средствами обработки информации, в том числе:

a) правила для электронной почты и интернет-пользователей (10.8);

b) рекомендации по использованию мобильных устройств, особенно для использования вне помещений организации (11.7.1).

Конкретные правила и рекомендации должны быть предоставлены соответствующим органом управления. Сотрудники, подрядчики и пользователи сторонних организаций, использующие или имеющие доступ к активам организации, должны знать о существующих лимитах, установленных для их использования, связанными со средствами обработки информации и ресурсами. Они должны нести ответственность за их использование любыми ресурсами обработки информации, и любое такое использование осуществляется под их ответственность.

7.2 Классификация информации

Цель: Обеспечение уверенности в том, что информационные активы защищены на надлежащем уровне.

Информацию следует классифицировать, чтобы определить ее приоритетность, необходимость и степень ее защиты.

Информация имеет различные степени чувствительности и критичности. Некоторые виды информации могут требовать дополнительного уровня защиты или специальных методов обработки. Систему классификации информации следует использовать для определения соответствующего множества уровней защиты и потребности в специальных методах обработки.

7.2.1 Основные принципы классификации

Контроль

Информация должна классифицироваться исходя из правовых требований, ее конфиденциальности, а также ценности и критичности для организации.

Руководство по внедрению

При классификации информации и связанных с ней мероприятий по управлению информационной безопасностью следует учитывать требования бизнеса в совместном использовании и ограничении доступа к информации, а также последствия, связанные с такими требованиями, например, неавторизованный доступ или повреждение информации.

Принципы классификации должны включать соглашения по первоначальной классификации и переклассификации в течение всего времени, в соответствии с заданной политикой контроля доступа (11.1.1).

Владелец должен нести ответственность (7.1.2) за определение классификации актива, периодически пересматривать и обеспечивать ее постоянное обновление на соответствующем уровне. Классификация должна принять во внимание «эффект накопления», приведенное в 10.7.2.

Следует принять во внимание число категорий классификации и преимущества от их использования. Чрезмерно сложные схемы категорирования информации могут стать обременительными и неэкономичными для использования или оказываются неосуществимыми. Следует проявлять осмотрительность при интерпретации категорий (грифов) классификации на документах от других организаций, которые могут иметь другие определения или содержание для тех же самых или подобных категорий.

Прочая информация

Степень защиты может оцениваться путем анализа конфиденциальности, целостности и доступности, а также любыми другими требованиями к рассматриваемой информации.

Информация обычно перестает быть чувствительной или критичной к компрометации по истечении некоторого периода времени, например, когда она становится общедоступной. Эти аспекты следует принимать во внимание, поскольку присвоение повышенной категории может вести к ненужным дополнительным расходам.

Рассмотрев документы с аналогичными требованиями безопасности, а также в присвоении категорий (грифов) классификации могло бы помочь в упрощении задач классификации.

В общем, классификация информации позволяет определить, как эта информация должна быть обработана и защищена.

7.2.2 Маркировка и обработка информации

Контроль

В соответствии с принятой в организации системой классификации должна быть разработана и реализована совокупность процедур маркировки и обработки информации.

Руководство по внедрению

Процедуры для маркировки и обработки информации должны относиться к информационным активам, представленным как в физической, так и в электронной форме.

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

Для каждой классификации должны быть определены процедуры обработки для того, чтобы учесть типы обработки информации, как безопасная обработка, хранение, передача, рассекречивание и уничтожение. Также должны быть включены процедуры по обеспечению сохранности и регистрации записей о событиях, связанных с безопасностью.

Соглашения с другими организациями, которые включают обмен информацией должны быть предусмотрены процедуры определения классификации этой информации и интерпретацию категорий (грифов) информации других организаций.

Прочая информация

Маркировка и безопасная обработка важной информации является ключевым требованием в соглашении для обмена информацией. Физические метки являются, в общем случае, наиболее подходящей формой маркировки. Однако некоторые информационные активы, такие как документы в электронной форме, физически не могут быть промаркированы, и поэтому необходимо использовать электронные аналоги маркировки. Например, маркировка уведомлений может появиться на экране монитора. Где маркировка невозможна, могут применяться другие средства обозначения классификации информации, например, через процедуры или метаданные.

8 Правила безопасности, связанные с персоналом

8.1 Перед трудоустройством [2)]

Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и пользователи сторонней организации осознают свою ответственность и способны выполнять предусмотренные для них функции и снижать риск от воровства, мошенничества и нецелевого использования оборудования, а также от угроз безопасности информации.

Ответственность за обеспечение безопасности определяется до трудоустройства в соответствующих должностных инструкциях, а также в сроки и на условиях при приеме на работу.

Все кандидаты на работу, подрядчики и пользователи сторонней организации должны проходить тщательный отбор, особенно это касается должностей, предполагающих доступ к важной информации.

Все сотрудники и представители сторонних организаций, использующие средства обработки информации организации, должны подписать соглашение о своих функциях и обязанностях в области информационной безопасности.

8.1.1 Функции и обязанности персонала по обеспечению безопасности

Контроль

Функции и обязанности персонала по обеспечению безопасности сотрудников, подрядчиков и пользователей третьих сторон в области безопасности должны быть определены и документированы в соответствии с требованиями информационной безопасности.

Руководство по внедрению

Функции и обязанности персонала по обеспечению безопасности должны содержать следующие требования:

a) внедрять и действовать в соответствии с политикой информационной безопасности (5.1);

b) защищать ресурсы от несанкционированного доступа, раскрытия, изменения, уничтожения или создания препятствий для их использования;

c) выполнять определенные процессы и мероприятия, связанные с безопасностью;

d) гарантировать выполнения обязанностей, порученных отдельным лицам при выполнении работ;

e) предоставлять отчеты о событиях безопасности или других рисках безопасности.

[2)] Значение слова «трудоустройство» (employment) здесь поняты следующие ситуации: прием на работу (временную или постоянную), назначение на должность или перевод на другую должность, переоформление контрактов или аннулирование каких-либо из этих ситуаций.

Функции и обязанности персонала по обеспечению безопасности, должны быть четко определены и сообщены кандидатам при приеме на работу, в ходе предварительного процесса трудоустройства.

Прочая информация

Функции и обязанности персонала должны быть документированы в должностных инструкциях. Работники не занятые в рабочем процессе организации, например, работающие в сторонней организации, также функции и обязанности, должны быть четко определены и уведомлены.

8.1.2 Проверка при приеме на работу

Контроль

Проверка всех кандидатов на постоянную работу, подрядчиков и пользователей сторонней организации должна быть проведена в соответствии с законами, инструкциями и правилами этики, с учетом требований бизнеса, характера информации к которой будет осуществлен их доступ, и предполагаемых рисков.

Руководство по внедрению

Проверки сотрудников, принимаемых в постоянный штат по мере подачи заявлений о приеме на работу, следует соблюдать конфиденциальность личных данных, в соответствии с действующим трудовым законодательством. В них необходимо включать следующее:

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

b) проверка (на предмет полноты и точности) резюме претендента;

c) подтверждение заявляемого образования и профессиональных квалификаций;

d) независимая проверка подлинности документа, удостоверяющих личность (паспорт или заменяющего его документа);

e) более детальная «проверка на доверие», такая как проверка по кредиту или на судимость.

В случаях, когда новому сотруднику непосредственно после приема на работу или в ее процессе предстоит доступ к средствам обработки важной информации, например финансовой или совершенно секретной информации организации, следует выполнить специальную «проверку на доверие».

Процедуры должны определить критерии и ограничения для проведения проверок, например, кто имеет право на проверку кандидатов на работу, и как, когда и почему контрольные проверки проводятся.

Аналогичный процесс проверки следует осуществлять для подрядчиков и временного персонала. В тех случаях, когда прием сотрудников осуществляется через кадровое агентство, контракт с агентством должен четко определять обязанности агентства по проверке претендентов и процедурам уведомления, которым оно должно следовать, если проверка не была закончена или если результаты дают основания для сомнения или беспокойства. В контракте со сторонней организацией должны быть четко определены (6.2.3) все функции и процедуры уведомления для проведения проверки.

Информация о всех рассматриваемых кандидатов, принимаемых в постоянный штат должна быть собрана и обработана в соответствии с действующим законодательством в пределах компетенции. В зависимости от применяемого законодательства, кандидаты должны быть заранее проинформированы о процедурах проверки.

8.1.3 Условия трудового договора

Контроль

Сотрудники, подрядчики и пользователи сторонней организации должны согласовать и подписать условия трудового договора, в котором установлены их

ответственность и ответственность организации относительно информационной безопасности.

Руководство по внедрению

Сроки и условия трудового договора должны отражать политику безопасности организации, в дополнение к разъяснению и заявлению:

a) для получения доступа к важной информации, все сотрудники, подрядчики и пользователи сторонних организаций, должны подписать соглашение о соблюдении конфиденциальности и неразглашении до предоставления доступа к средствам обработки информации;

b) ответственность и права сотрудников, подрядчиков и любых других пользователей, относительно законов об авторском праве или по защите данных (15.1.1 и 15.1.2);

c) ответственность за классификацию информации и управление активами организации, связанными с информационными системами и услугами, обрабатываемыми сотрудниками, подрядчиками или пользователями сторонних организаций (7.2.1 и 10.7.3);

d) ответственность сотрудников, подрядчиков или пользователей сторонней организации за обработку информации, полученную от других компаний или организаций;

e) ответственность организации за обработку персональной информации, включая информацию, созданную в результате работы в организации (15.1.4);

f) ответственность распространяется и на работу вне помещений организации, и вне рабочее время, например, в случае исполнения работы на дому (9.2.5 и 11.7.1);

g) необходимо предпринять соответствующие меры, если сотрудник, подрядчик или пользователь сторонней организации, игнорирует требования безопасности в организации (см. 8.2.3).

Организация должна согласовать с сотрудниками, подрядчиками и пользователями сторонних организаций условия и правила пользования, касающиеся информационной безопасности с учетом характера и степени доступа к активам организации, связанных с информационными системами и услугами.

Там, где необходимо, эта ответственность должна сохраняться и в течение определенного срока после увольнения с работы (8.3).

Прочая информация

Необходимо использовать свод правил по вопросам ответственности сотрудников, подрядчиков или пользователей сторонних организаций в отношении конфиденциальности, защиты данных, правил этики и соответствующего использования оборудования организации и объектов, так же как достойных действий ожидаемых со стороны организации. Подрядчики или пользователи третьей стороны могут быть связаны со сторонними организациями, которые могут в свою очередь ввести в контрактные соглашения от имени лица, вовлеченного в контракт.

8.2 Работа по трудовому договору

Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и пользователи сторонней организации осведомлены об угрозах и проблемах информационной безопасности, об их ответственности и обязательствах, ознакомлены с правилами и обучены процедурам для поддержания мер безопасности организации при выполнении ими своих служебных обязанностей и для снижения риска человеческого фактора для информационной безопасности.

Обязанности руководства должны быть определены для обеспечения безопасности применяемые к каждому сотруднику в организации.

Адекватный уровень осведомленности, обучения и подготовки кадров в области

безопасности и правильное использование средств обработки информации, должны предоставляться всем сотрудникам, подрядчикам или пользователям сторонних организаций, чтобы свести к минимуму возможные риски безопасности. А также необходимо применить дисциплинарную практику в процессе нарушения требований безопасности.

8.2.1 Обязанности руководства

Контроль

Руководство организации должно требовать, чтобы сотрудники, подрядчики и пользователи сторонней организации были ознакомлены с правилами и процедурами обеспечения мер безопасности в соответствии с установленными требованиями.

Руководство по внедрению

В обязанности руководства входят обеспечение того, чтобы сотрудники, подрядчики и пользователи сторонних организаций:

a) были осведомлены об их информационной безопасности, функциях и обязанностях до предоставления доступа к конфиденциальной информации или информационным системам;

b) получили руководства пользователя в области политики безопасности для определения ожидаемых результатов их функций в организации;

c) были мотивированы для выполнения политики безопасности организации;

d) достигли уровня информированности по вопросам безопасности, имеющие отношение к своим функциям и обязанностям в рамках организации (см. 8.2.2);

e) соответствовали условиям трудовой деятельности, которая включает в себя политику информационной безопасности в организации, а также соответствующие методы работы;

f) имели соответствующие навыки и квалификацию.

Прочая информация

Если сотрудники, подрядчики или пользователи сторонних организаций не осведомлены о своих обязанностях по обеспечению безопасности, то они могут причинить значительный ущерб организации. Мотивированный персонал может быть более надежным и привести к сокращению числа инцидентов нарушения информационной безопасности.

Руководство не соответствующее занимаемой должности может вызвать у персонала ощущение своей недооценки и привести к негативному воздействию на безопасность в организации. Например, подобное несоответствие может привести к пренебрежению безопасностью сотрудниками или злоупотреблению активами организации.

8.2.2 Осведомленность, обучение и переподготовка в области информационной безопасности

Контроль

Все сотрудники организации и, при необходимости, подрядчики и пользователи сторонних организаций должны проходить соответствующее обучение и переподготовку в целях регулярного получения информации о новых требованиях правил и процедур организации безопасности, необходимых для выполнения ими должностных функций.

Руководство по внедрению

Соответствующее обучение следует начинать с ознакомления политикой информационной безопасности в организации до предоставления доступа к информации и услугам.

Обучение сотрудников должно обеспечить знание ими требований безопасности, ответственности в соответствии с законодательством, мероприятий по управлению информационной безопасностью, а также знание правильного использования средств

обработки информации, например, процедур регистрации в системах, использования пакетов программ и информации относительно дисциплинарной практики (см. 8.2.3).

Прочая информация

Деятельность по обучению и подготовки в области безопасности должна соответствовать функциям сотрудника, его ответственности и навыкам, а также должна содержаться информация об известных угрозах. Сотруднику в случае необходимости, следует обращаться за консультацией специалисту по вопросам безопасности и надлежащих каналов для оповещения об инцидентах нарушения информационной безопасности (13.1).

Необходима подготовка в целях повышения осведомленности, информирования и процедурах реагирования на инциденты в соответствии с потребностями их функции работы.

8.2.3 Дисциплинарная практика

Контроль

К сотрудникам совершившим нарушение требований безопасности, должна быть применена дисциплинарная практика, установленная в организации.

Руководство по внедрению

Дисциплинарная практика не должна применяться без предварительной проверки при нарушении безопасности (см. 13.2.3 для сбора доказательств).

Применение дисциплинарной практики обеспечит корректное и справедливое рассмотрение для сотрудников, которые подозреваются в серьезных или регулярных нарушениях требований безопасности. Применение официальной дисциплинарной практики должно обеспечить постепенное реагирование, принимающее во внимание такие факторы, как характер и степень тяжести нарушения и его воздействия на бизнес, было ли это нарушение совершено впервые или нарушалось неоднократно, получал ли нарушитель достаточное обучение, соответствующее законодательству, трудовому соглашению или другим факторам, по мере необходимости. В случаях серьезных проступков, применение дисциплинарной практики должно позволить снятие с занимаемой должности, лишение права доступа и привилегий, а также в случае необходимости, немедленного освобождения рабочего места.

Прочая информация

Дисциплинарная практика также должна применяться в качестве сдерживающего фактора для предотвращения нарушений политики и процедур по обеспечению безопасности или любых других нарушений безопасности со стороны сотрудников, подрядчиков и сторонних организаций.

8.3 Прекращение или изменение действия трудового договора

Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и пользователи сторонней организации уведомлены об увольнении или изменении условий трудового договора в соответствии с установленным порядком.

Необходимо назначить ответственного по обеспечению возврата всего оборудования и устранения всех прав доступа после увольнения сотрудника, подрядчика или пользователя сторонней организации.

Изменение обязанностей и функций в организации должны быть управляемыми, как прекращение соответствующей ответственности или работы по трудовому договору в соответствии с настоящим разделом, и любые новые функции должны управляться, как описано в Разделе 8.1.

8.3.1 Ответственность по окончании действия трудового договора

Контроль

Ответственность по окончании действия трудового договора должна быть четко определена и установлена.

Руководство по внедрению

Информация об ответственности, по окончании действия трудового договора, должна включать текущие требования к безопасности и правовую ответственность, и при необходимости, обязанностей, содержащихся в любом соглашении о конфиденциальности (см. 6.1.5). А также сроки и условия трудового договора (8.1.3) должны действовать в течение определенного периода времени после завершения срока работы сотрудников, подрядчиков или пользователей сторонней организации.

Функции и обязанности остаются в силе после прекращения работы, которые указаны в трудовых соглашениях сотрудников, подрядчиков или пользователей сторонней организации.

Изменение обязанностей или функций должны быть управляемыми, как прекращение соответствующей ответственности или работы по трудовому договору, а также новые обязанности или функции должны контролироваться, как описано в 8.1.

Прочая информация

В функцию персонала входит, как правило, ответственность за общий процесс после окончания действия трудового договора и совместной работы с контролирующими менеджерами, оставляя сотруднику обеспечение управления безопасностью всеми соответствующими аспектами процедур. В случае с подрядчиком, этот процесс прекращения ответственности, может осуществляться органом, ответственным за подрядчиков, и в случае других пользователей этим может заниматься их организация.

Необходимо информировать сотрудников, заказчиков, подрядчиков или пользователей сторонней организаций об изменениях в рабочем процессе и в работе с персоналом.

8.3.2 Возврат активов

Контроль

Сотрудники, подрядчики и пользователи сторонней организации обязаны вернуть все активы организации, находящиеся в их пользовании (владении), по истечении срока действия трудового договора или соглашения (увольнения).

Руководство по внедрению

Процесс увольнения должен быть формализован включая возвращение всех ранее выпущенных программ, служебных документов и оборудования. Прочие активы организации, такие как, мобильные вычислительные устройства, кредитные карты, карты доступа, программное обеспечение, руководства и информация, хранящаяся на электронных носителях, также должны быть возвращены.

Если сотрудник, подрядчик или пользователь сторонней организации приобретает оборудование организации или использует личное оборудование, то процедуры должны осуществляться для обеспечения того, чтобы вся соответствующая информация была передана организации или надежно удалена с оборудования (см. 10.7.1).

В случаях, когда сотрудник, подрядчик или пользователь сторонней организации, знает, что это важно для текущих операций, то эта информация должна быть задокументирована и передана организации.

8.3.3 Аннулирование прав доступа

Контроль

Права доступа к информации и средствам обработки информации сотрудников, подрядчиков и пользователей сторонней организации должны быть аннулированы или уточнены по окончании действия трудового договора (увольнение).

Руководство по внедрению

По окончании действия трудового договора (увольнения), права доступа к отдельным активам, связанных с информационными системами и услугами должны быть пересмотрены. При этом определяется необходимость аннулирования прав доступа. Изменения в работе должны быть отражены в аннулировании всех прав доступа, которые не были утверждены для новой работы. Права доступа, которые должны быть аннулированы или адаптированы, включают физический и логический доступ, ключи, идентификационные карты, средства обработки информации (см. 11.2.4), подписки, и удаления из всей документации, которая идентифицирует их в качестве действительного члена этой организации. Если уволившийся сотрудник, подрядчик или пользователь сторонней организации знает пароли для учетных записей, оставшихся активными, то пароли должны быть изменены на момент прекращения или изменения работы, окончания действия трудового договора или соглашения.

Права доступа к информационным активам и средствам обработки информации должны быть сокращены или аннулированы, прежде чем действие трудового договора прекращается или изменяется в зависимости от оценки факторов риска, таких как:

a) является ли прекращение или изменение по инициативе сотрудника, подрядчика или пользователя сторонней организации, или по инициативе руководства и какова причина прекращения;

b) текущие обязанности сотрудника, подрядчика или любых других пользователей;

c) ценность активов, доступных в настоящее время.

Прочая информация

При определенных обстоятельствах, правами доступа может воспользоваться большое количество людей, чем уволившийся сотрудник, подрядчик или пользователь сторонней организации, например, групповых ID. При таких обстоятельствах, уволившиеся лица должны быть аннулированы из всех списков группового доступа, а также сотрудникам, подрядчикам или пользователям сторонней организации рекомендуется не обмениваться информацией с увольняющимися лицами.

В случае прекращения действия трудового договора (увольнения) по инициативе руководства, недовольные сотрудники, подрядчики или пользователи сторонней организации, могут преднамеренно повредить информацию или саботировать средства обработки информации. Уволившиеся лица могут произвести попытку собрать информацию для будущего использования.

9 Физическая защита и защита от воздействия окружающей среды

9.1 Охраняемые зоны

Цель: Предотвращение несанкционированного физического доступа, повреждения и воздействия на помещения и информацию организации.

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

Уровень защищенности должен быть соразмерен с определенными рисками.

9.1.1 Периметр физической безопасности

Контроль

Для защиты зон, где имеются информация и средства обработки информации, должны быть использованы периметры охраняемых зон (барьеры, такие как стены,

проходные, оборудованные средствами контроля входа по идентификационным карточкам, или, где предусмотрен контроль сотрудника регистрационной стойки).

Руководство по внедрению

Рекомендуется рассматривать и внедрять при необходимости следующие мероприятия по обеспечению информационной безопасности:

a) периметр безопасности должен быть четко определен, расположение и прочность каждого из периметров зависит от требований безопасности активов в периметре безопасности и результатов оценки рисков;

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

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

d) физические барьеры, в случае необходимости, должны быть расширены от пола до потолка, для предотвращения неавторизованных проникновений, а также исключения загрязнения окружающей среды в случае пожара или затоплений;

e) все противопожарные выходы в периметре безопасности должны быть оборудованы аварийной сигнализацией и плотно закрываться, в соответствии с действующими нормативными документами и нормами противопожарной безопасности;

f) при необходимости устанавливать соответствующие системы обнаружения против взлома в соответствии с действующими нормативными документами и регулярно проводить их испытания с охватом всех наружных дверей и окон; в неохраняемых зонах постоянно должна работать сигнализация; другие зоны, например, компьютерные комнаты или комнаты связи также должны быть обеспечены защитой;

g) средства обработки информации, которыми управляет организация должны быть физически отделены от средств обработки информации, которыми управляют сторонние организации.

Прочая информация

Физическая защита может быть достигнута созданием нескольких физических барьеров (преград) вокруг помещений организации и средств обработки информации. Использование нескольких барьеров дает дополнительную защиту там, где повреждение одного барьера не означает появления риска для безопасности.

Зона информационной безопасности может быть защищена путем закрытия на замок самого офиса или нескольких помещений внутри физического периметра безопасности. Внутри одного периметра безопасности могут потребоваться дополнительные барьеры и физические периметры для контроля доступа.

В зданиях, где расположены несколько офисов, должны предусматриваться особые способы обеспечения физической защиты.

9.1.2 Контроль доступа в охраняемую зону

Контроль

Зону информационной безопасности необходимо защищать с помощью соответствующих мер контроля входа для обеспечения уверенности в том, что доступ позволен только авторизованному персоналу.

Руководство по внедрению

Необходимо рассматривать следующие меры контроля:

a) посетители зон безопасности должны сопровождаться или обладать соответствующим допуском; дату и время входа и выхода следует регистрировать. Доступ следует предоставлять только для выполнения определенных авторизованных задач. Необходимо также знакомить посетителей с требованиями безопасности и действиями на случай аварийных ситуаций;

b) доступ к важной информации и средствам ее обработки должен контролироваться и предоставляться только авторизованным лицам. Следует использовать средства аутентификации, например, карты доступа плюс PIN-код для авторизации и предоставления соответствующего доступа. Необходимо также надлежащим образом проводить аудит журналов регистрации доступа;

c) необходимо требовать, чтобы весь персонал носил признаки видимой идентификации, следует поощрять его внимание к незнакомым несопровождаемым посетителям, не имеющим идентификационных карт сотрудников;

d) посетители со стороны персонала службы получают ограниченный доступ к важной информации и средствам ее обработки, только в случае необходимости; для такого доступа требуется разрешение и ведение наблюдения;

e) права доступа сотрудников в зоны информационной безопасности следует регулярно анализировать и пересматривать (8.3.3).

9.1.3 Обеспечение безопасности зданий, производственных помещений и оборудования

Контроль

Для обеспечения безопасности зданий, производственных помещений и оборудования должны быть разработаны и реализованы физические меры защиты.

Руководство по внедрению

Необходимо рассматривать следующие меры для обеспечения безопасности зданий, помещений и оборудования:

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

b) основное оборудование должно быть расположено в местах с ограничением доступа посторонних лиц;

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

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

9.1.4 Защита от внешних угроз и угроз со стороны окружающей среды

Контроль

При выборе и проектировании безопасной зоны следует принимать во внимание возможные последствия от пожара, наводнения, землетрясения, взрыва, уличных беспорядков и других форм природного или искусственного бедствия.

Руководство по внедрению

Необходимо рассматривать также любые угрозы безопасности от соседних помещений, например, протекание крыши, затоплений или пожара на улице:

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

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

c) следует обеспечить противопожарным оборудованием, размещенным в доступном месте.

9.1.5 Выполнение работ в охраняемых зонах

Контроль

Для повышения степени защиты зон информационной безопасности могут потребоваться дополнительные меры по управлению информационной безопасностью и соответствующие руководства.

Руководство по внедрению

Необходимо рассматривать следующие мероприятия, работающих в зоне безопасности:

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

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

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

d) использование фото, видео, аудио или другого записывающего оборудования, цифровых камер в мобильных устройствах должно быть разрешено только при получении специального разрешения;

Подготовка к работе в безопасных зонах должны включать мероприятия в отношении персонала или представителей третьих сторон, работающих в зоне безопасности зоне.

9.1.6 Зоны общественного доступа, приема и отгрузки материальных ценностей

Контроль

Зона приемки и отгрузки материальных ценностей должны находиться под контролем, и по возможности, быть изолированы от средств обработки информации во избежание неавторизованного доступа.

Руководство по внедрению

Необходимо рассматривать следующие мероприятия:

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

b) зона складирования 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 внешней двери помещения для складирования, когда внутренняя дверь открыта;

d) поступающие материальные ценности должны быть осмотрены на предмет потенциальных опасностей (9.2.1 d) прежде, чем они будут перемещены из помещения для складирования к местам использования;

e) поступающие материальные ценности должны быть зарегистрированы при входе в помещение, в соответствии с процедурами управления активами (7.1.1);

f) приемка и отгрузка материальных ценностей должна быть отдельна, если это необходимо.

9.2 Безопасность оборудования

Цель: Предотвращение потерь, повреждений или компрометаций активов и

нарушения непрерывности деятельности организации.

Необходимо обеспечивать безопасность оборудования (включая и то, что используется вне организации), чтобы уменьшить риск неавторизованного доступа к данным и защитить их от потери или повреждения. При этом необходимо принимать во внимание особенности, связанные с расположением оборудования и возможным его перемещением. Могут потребоваться специальные мероприятия от опасных воздействий среды или неавторизованного доступа через инфраструктуры обеспечения, в частности, системы электропитания и кабельной разводки.

9.2.1 Размещение и защита оборудования

Контроль

Оборудование должно быть расположено и защищено так, чтобы уменьшить риск от воздействий окружающей среды и возможности неавторизованного доступа.

Руководство по внедрению

Необходимо рассматривать следующие мероприятия по управлению информационной безопасностью:

a) оборудование необходимо размещать таким образом, чтобы свести до минимума излишний доступ в места его расположения;

b) средства обработки и хранения важной информации следует размещать так, чтобы, уменьшить риск несанкционированного наблюдения за их функционированием;

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

d) меры по управлению информационной безопасностью должны свести к минимуму риск потенциальных угроз, например, воровство, пожар, взрыв, задымление, затопление (или перебои в подаче воды), пыль, вибрация, химические воздействия, помехи в электроснабжении, помехи связи, электромагнитное облучение, вандализм;

e) в организации следует определить порядок приема пищи, напитков и курения вблизи средств обработки информации;

f) следует проводить мониторинг состояния окружающей среды в целях выявления условий (температура, влажность), которые могли бы неблагоприятно повлиять на функционирование средств обработки информации;

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

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

i) оборудование для обработки важной информации должно быть защищено с целью свести к минимуму риск по утечке информации, вследствие электромагнитного излучения.

9.2.2 Вспомогательные услуги

Контроль

Оборудование необходимо защищать от перебоев в подаче электроэнергии и других сбоев, связанных с отказами в обеспечении вспомогательных услуг.

Руководство по внедрению

Все вспомогательные услуги, такие как электричество, водоснабжение, канализация, отопление, вентиляция и кондиционирование, должны соответствовать системам, для которых они предназначены. Все инженерные системы и их оборудования должны регулярно осматриваться и соответствующим образом тестироваться для обеспечения их надлежащего функционирования и сокращения риска вследствие их неисправности или сбоя. Также необходимо обеспечить подходящее энергоснабжение, соответствующее техническим характеристикам от производителя оборудования.

Чтобы обеспечить безопасное выключение и/или непрерывное функционирование устройств, поддерживающих критические бизнес-процессы, рекомендуется подключать оборудование через UPS. В планах обеспечения непрерывности следует предусматривать действия, которые должны быть предприняты при отказе UPS. Резервный генератор следует применять, если необходимо обеспечить функционирование оборудования в случае длительного отказа подачи электроэнергии от общего источника. Для бесперебойной работы генератора в течение длительного срока необходимо обеспечить соответствующую поставку топлива. Оборудование UPS и генераторы следует регулярно проверять на наличие адекватной мощности, а также тестировать в соответствии с рекомендациями производителя.

Кроме того, можно рассмотреть возможность использования нескольких источников энергии в помещениях отдельно стоящей подстанции.

Аварийные выключатели электропитания необходимо располагать около запасных выходов помещений, где расположено оборудование, чтобы ускорить отключение электропитания в случае критических ситуаций. Следует обеспечить работу аварийного освещения на случай отказа электропитания, потребляемого от сети.

Система водоснабжения должна быть стабильной и приемлемой для

- обеспечения кондиционирования воздуха;
- увлажнения воздуха (при необходимости);
- оборудования систем пожаротушения.

Неисправности в системе водоснабжения могут повредить оборудование или создать помехи для эффективной работы систем пожаротушения. При необходимости устанавливается автоматическая система обнаружения неисправностей в системе водоснабжения.

Телекоммуникационное оборудование должно быть подключено к системным поставщикам, по крайне мере двумя разными маршрутами, чтобы предотвратить отказ одного канала подключения услуги телефонии. Услуги телефонии должны удовлетворять и соответствовать нормативным требованиям аварийной связи.

Прочая информация

Для достижения непрерывности подачи электропитания необходимо наличие нескольких источников электропитания, чтобы избежать последствия при нарушении его подачи от единственного источника.

9.2.3 Безопасность кабельной сети

Контроль

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

Руководство по внедрению

Необходимо рассматривать следующие мероприятия:

а) силовые и телекоммуникационные линии, связывающие средства обработки информации, должны быть, по возможности, подземными или обладать адекватной альтернативной защитой;

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

с) силовые кабели должны быть отделены от коммуникационных, чтобы исключить помехи;

д) четко определенная маркировка кабелей и оборудования должна быть использована для минимизации обработки ошибки, такие как неправильно выбранные сетевые кабели;

e) документы со списком обновлений, должны быть использованы для уменьшения вероятности ошибок;

f) дополнительные мероприятия по управлению информационной безопасностью для чувствительных или критических систем включают:

1) использование бронированных кожухов, а также закрытых помещений/ящиков в промежуточных пунктах контроля и конечных точках;

2) использование дублирующих маршрутов прокладки кабеля или альтернативных способов передачи;

3) использование оптико-волоконных линий связи;

4) использование электромагнитного экранирования для защиты кабелей;

5) инициирование технических зачисток и физических осмотров для несанкционированных устройств присоединенных к кабелям;

6) ограничение доступа к соединительным панелям и кабельным линиям.

9.2.4 Техническое обслуживание оборудования

Контроль

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

Руководство по внедрению

В этих целях следует применять следующие мероприятия:

a) оборудование следует обслуживать в соответствии с инструкциями и периодичностью, рекомендуемыми поставщиком;

b) необходимо, чтобы техническое обслуживание и ремонт оборудования проводились только авторизованным персоналом;

c) следует хранить записи обо всех предполагаемых или фактических неисправностей и всех видах профилактического и восстановительного технического обслуживания;

d) необходимо принимать соответствующие меры безопасности при отправке оборудования для технического обслуживания за пределы организации в отношении удаленных, стертых и перезаписанных данных;

e) необходимо соблюдать все требования, устанавливаемые использующимися правилами страхования.

9.2.5 Обеспечение безопасности оборудования, используемого вне помещений организации

Контроль

Уровень информационной безопасности должен быть эквивалентен уровню безопасности в отношении оборудования, используемого с аналогичной целью в помещениях организации, а также с учетом рисков работы на стороне.

Руководство по внедрению

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

Необходимо применять следующие мероприятия по управлению информационной безопасностью:

a) оборудование и носители информации, взятые из помещений организации, не следует оставлять без присмотра в общедоступных местах. При перемещении компьютеры следует перевозить как ручную кладь и, по возможности, не афишировать ее содержимое;

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

c) при работе дома следует применять подходящие мероприятия по управлению информационной безопасностью с учетом оценки рисков, например, использовать

запираемые файл-кабинеты, соблюдать политику «чистого стола» и контролировать возможность доступа к компьютерам (см. СТ РК ИСО/МЭК 18028-4);

d) должны иметь место адекватные меры по страхованию для защиты оборудования вне помещений организации.

Риски безопасности, например, связанные с повреждением, воровством и подслушиванием, могут в значительной степени зависеть от расположения оборудования в организации и должны учитываться при определении и выборе наиболее подходящих мероприятий по управлению информационной безопасностью.

Прочая информация

Оборудования по обработке и хранению информации включает все типы персональных компьютеров, электронных записных книжек, мобильных телефонов, смарт-карты, а также бумагу или иные материальные ценности, которые используются для работы на дому или транспортируются за пределы рабочих помещений.

Более подробная информация о других аспектах защиты мобильного оборудования, приведена в 11.7.1.

9.2.6 Безопасная утилизация (списание) или повторное использование оборудования

Контроль

Все компоненты оборудования, содержащего носители данных следует проверять на предмет удаления всех важных данных и лицензионного программного обеспечения.

Руководство по внедрению

Носители данных, содержащие важную информацию, необходимо физически разрушать или перезаписывать безопасным образом, а не использовать стандартные функции удаления.

Прочая информация

В отношении носителей данных, содержащих важную информацию, может потребоваться оценка рисков с целью определения целесообразности их разрушения, восстановления или выбраковки.

Служебная информация может быть скомпрометирована вследствие небрежной утилизации или повторного использования оборудования (10.7.2).

9.2.7 Вынос имущества

Контроль

Оборудование, информацию или программное обеспечение можно выносить из помещений организации только на основании соответствующего разрешения.

Руководство по внедрению

Следует рассматривать следующие мероприятия:

a) оборудование, информация или программное обеспечение не должны вывозиться за пределы организации без соответствующего разрешения.

b) должны быть четко определены права на вывоз активов за пределы помещений сотрудниками, подрядчиками или пользователями сторонних организаций;

c) необходимо установить лимит времени для вывоза оборудования и соблюдения условий возврата;

d) оборудование следует регистрировать при выносе и при вносе, а также делать отметку, когда оно возвращено.

Прочая информация

Выборочные проверки проводимые для обнаружения несанкционированного изъятия имущества, также могут быть выполнены для обнаружения несанкционированных записывающих устройств, оружия и т.д., и не допустить их въезда в здание**.** Такие выборочные проверки должны осуществляться в соответствии с действующим законодательством и правилам. Сотрудники должны быть осведомлены о

выборочной проверке, и эти проверки должны осуществляться только с разрешения в соответствии с правовыми и нормативными требованиями.

10 Управление передачей данных и операционной деятельностью

10.1 Операционные процедуры и обязанности

Цель: Обеспечить надлежащее и безопасное функционирование средств обработки информации.

Должны быть установлены обязанности и процедуры по управлению и функционированию всех средств обработки информации. Они должны включать разработку соответствующих операционных инструкций и процедуры реагирования на инциденты.

С целью минимизации риска при не правильном использовании систем вследствие небрежности или злого умысла следует, по возможности, реализовывать принцип разделения полномочий.

10.1.1 Документальное оформление операционных процедур

Контроль

Операционные процедуры должны документироваться, поддерживаться и быть доступными для авторизованных пользователей.

Руководство по внедрению

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

Процедуры содержат детальную инструкцию выполнения конкретного задания (работы) и включают:

a) обработку и управление информацией;

b) копирование (10.5);

c) определение требований в отношении графика выполнения заданий, включающих взаимосвязи между системами; время начала выполнения самого раннего задания и время завершения самого последнего задания;

d) обработку ошибок или других исключительных ситуаций, которые могут возникнуть в течение выполнения заданий, включая ограничения на использование системных утилит (11.5.4);

e) необходимые контакты на случай неожиданных операционных и технических проблем;

f) специальные мероприятия по управлению выводом данных, например, использование специальной бумаги для печатающих устройств или особых процедур применительно к выводу конфиденциальной информации, включая процедуры для безопасной утилизации выходных данных, не завершенных в процессе выполнения заданий (10.7.2 и 10.7.3);

g) перезапуск системы и процедуры восстановления в случае системных сбоев;

h) ведение журнала аудита и системного журнала регистрации (10.10).

Операционные процедуры, определяемые политикой безопасности, должны рассматриваться как официальные документы, документироваться и строго соблюдаться, а изменения к ним должны санкционироваться и утверждаться руководством. Там, где это технически возможно, информационные системы должны решаться последовательно, используя те же процедуры, инструменты и утилиты.

10.1.2 Контроль изменений

Контроль

Изменения в конфигурациях средств обработки информации и системах должны быть контролируемыми.

Руководство по внедрению

Процедуры управления изменениями в операционной среде и в программных приложениях должны быть интегрированы. В частности, необходимо рассматривать следующие мероприятия:

a) определение и регистрация существенных изменений;

b) планирование и тестирование изменений;

c) оценка возможных последствий таких изменений;

d) формализованная процедура утверждения предлагаемых изменений;

e) подробное информирование об изменениях всех заинтересованных лиц;

f) процедуры, определяющие обязанности по прерыванию и восстановлению работы средств и систем обработки информации, в случае неудачных изменений программного обеспечения.

С целью обеспечения надлежащего контроля для всех изменений в оборудовании, программном обеспечении или процедурах должны быть определены и внедрены формализованные роли, ответственности и процедуры. При изменении программного обеспечения вся необходимая информация должна фиксироваться и сохраняться в системном журнале аудита.

Прочая информация

Неадекватный контроль изменений средств и систем обработки информации – распространенная причина системных сбоев и инцидентов нарушения информационной безопасности. Изменения операционной среды могут оказывать влияние на работу приложений (12.5.1).

Изменения в операционных системах должны производиться при наличии уважительных причин при увеличении риска системы. Обновление системы с последними версиями операционных систем или приложений, не всегда в интересах бизнеса, поскольку это может ввести больше уязвимостей и нестабильности, чем в текущей версии. Также может возникнуть необходимость в дополнительном обучении, стоимости лицензий, поддержке, обслуживании и администрировании накладных расходов и новых аппаратных средств в период перемещения.

10.1.3 Разграничение обязанностей

Контроль

Обязанности и области ответственности должны быть разграничены в целях снижения возможностей несанкционированной или непреднамеренной модификации или нецелесообразного использования активов организации.

Руководство по внедрению

Разграничение обязанностей - способ минимизации риска нештатного использования систем вследствие ошибочных или злаономерных действий пользователей. Необходимо предпринимать меры предосторожности, чтобы сотрудник не мог использовать активы без авторизации или обнаружения. Инициирование события должно быть отделено от его авторизации. При мерах безопасности следует рассматривать возможность сговора.

Для небольших организаций эти мероприятия труднодостижимы, однако данный принцип должен быть применен на сколько это возможно. В случаях, когда разделение обязанностей осуществить затруднительно, следует рассматривать использование других мероприятий по управлению информационной безопасностью, таких как мониторинг

деятельности, использование журналов аудита, а также мер административного контроля. Важно, чтобы аудит безопасности оставался независимой функцией.

10.1.4 Разграничение средств разработки, тестирования и эксплуатации

Контроль

Средства разработки, тестирования и эксплуатации должны быть разграничены в целях снижения риска несанкционированного доступа или изменения операционной системы.

Руководство по внедрению

Следует обеспечивать необходимый уровень разделения между средами промышленной эксплуатации по отношению к средам тестирования, а также для предотвращения операционных сбоев. Необходимо рассматривать следующие мероприятия по управлению информационной безопасностью:

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

b) программное обеспечение для разработки и эксплуатации, по возможности, должно работать на различных компьютерных процессорах или в различных доменах или директориях;

c) компиляторы, редакторы и другие системные утилиты не должны быть доступны в операционной среде без крайней необходимости;

d) действия по разработке и тестированию должны быть разделены, насколько это возможно;

e) чтобы уменьшить риск ошибок, для операционных и тестовых систем должны использоваться различные процедуры регистрации (вход в систему), а в экранных меню должны показываться соответствующие идентификационные сообщения;

f) важные данные не следует копировать в тестовой системе (12.4.2).

Прочая 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 в рабочем состоянии отдельную среду, и в которой следует выполнять комплексное тестирование с известной стабильностью и предотвращать несанкционированный доступ со стороны разработчиков.

Там, где сотрудники, отвечающие за разработку и тестирование, имеют доступ к системе и данным среды промышленной эксплуатации, они имеют возможность установить неавторизованную и не протестированную программу или изменить данные в операционной среде. Применительно к ряду систем эта возможность могла бы быть использована с целью злоупотребления, а именно для мошенничества или установки не протестированной или вредоносной программы, что может быть причиной серьезных проблем в операционной среде.

Разработчики и специалисты, проводящие тестирование могут также быть причиной угроз для безопасности операционной информации и системы.

Кроме того, если разработка и тестирование производиться в одной компьютерной среде, это может стать причиной непреднамеренных изменений программного обеспечения или информации. Разделение средств разработки, тестирования и эксплуатации является, целесообразным для уменьшения риска случайного изменения или несанкционированного доступа к программному обеспечению и бизнес-данным среды промышленной эксплуатации (см. 12.4.2 для защиты данных тестирования системы).

10.2 Управление поставкой услуг лицами и/или сторонними организациями

Цель: Реализовать и поддерживать требуемый уровень информационной безопасности и оказания услуг в соответствии с договорами об оказании услуг сторонними организациями (внешними лицами и/или организациями).

Организация должна осуществлять контроль за выполнением, соблюдением соглашений, и управлять изменениями для того, чтобы оказываемые услуги удовлетворяли все требования, согласованные с третьей стороной.

10.2.1 Оказание услуг

Контроль

Должна быть обеспечена уверенность в том, что меры управления информационной безопасности, включенные в договор об оказании услуг сторонней организации, реализованы, функционируют и поддерживаются сторонней организацией.

Руководство по внедрению

В оказание услуг сторонней организации должна включать в себя согласованные меры безопасности, определения сервиса, а также аспекты управления услугами. В случае привлечения внешних подрядчиков, организация должна планировать необходимые переходы (информации, средств обработки информации, и все остальное, что должно быть перемещено), а также обеспечить безопасность и сохранность на протяжении периода перемещения.

Организация должна обеспечить сторонней организации сохранность достаточного потенциала службы вместе с существующими планами, направленными на обеспечение того, чтобы согласованные уровни непрерывного обслуживания велись и после эксплуатационных отказов, вызванных стихийными бедствиями или нарушениями безопасности (см. 14.1).

10.2.2 Мониторинг и анализ услуг, оказываемых сторонними лицами и/или организациями

Контроль

Необходимо регулярно проводить мониторинг, аудит и анализ услуг, отчетов и актов, обеспечиваемых сторонней организацией.

Руководство по внедрению

Мониторинг и анализ услуг, оказываемые сторонними организациями должны обеспечить безопасность информации и соблюдения условия соглашений и что инциденты нарушения информационной безопасности и проблемы, связанные с безопасностью, управляются соответствующим образом. Это должно касаться в отношении управленческих услуг и процесса между организацией и сторонними лицами:

а) следить за уровнем производительности службы с целью проверки соблюдения соглашений;

б) услуги по рассмотрению докладов, подготовленных сторонними лицами, и проведения регулярных совещаний, как предусмотрено в требованиях соглашений;

с) предоставлять информацию об инцидентах нарушения информационной безопасности и анализ этой информации сторонними лицами и организацией в соответствии с требованиями соглашений, и любые дополнительные рекомендации и процедуры;

d) проводить аудит и анализ услуг, отчетов о событиях безопасности, операционных проблем, неудач, отслеживания ошибок и сбоев, связанных с услугой поставки, обеспечиваемых сторонней организацией;

е) устранение и решение любых выявленных проблем.

Ответственность за управление отношениями со сторонней организацией, следует возложить на отдельных сотрудников или подразделений службы управления. Кроме того, организация должна обеспечить, чтобы сторонняя организация возлагала ответственность за проверку соблюдения и обеспечения соблюдения требований соглашений. Достаточные технические навыки и ресурсы должны быть доступными, чтобы контролировать требования соглашений (см. 6.2.3), в особенности информационные требования

безопасности. Должны быть приняты соответствующие меры при нарушении предоставленных услуг.

Организация должна поддерживать достаточный повсеместный контроль и отслеживать все аспекты безопасности важных и критических информаций или средств обработки информации, доступ перерабатывающих мощностей, переработанных или управляемых сторонней организацией. Организация должна обеспечить им сохранность и безопасность таких мероприятий, как управление преобразованиями, выявления уязвимостей и инцидентов информационной безопасности, оповещения/восстановления через четко определенные процедуры отчетности, формата и структуру.

Прочая информация

В случае привлечения внешних ресурсов, организацию необходимо известить о том, что полную ответственность за информацию, обработанную привлеченными внешними ресурсами, несет организация.

10.2.3 Изменения при оказании сторонними организациями услуг по обеспечению безопасности

Контроль

Изменения при оказании услуг по обеспечению безопасности, включая внедрение и совершенствование существующих требований, процедур и мер обеспечения информационной безопасности, должны быть управляемыми с учетом оценки критичности систем и процессов бизнеса, а также результатов переоценки рисков.

Руководство по внедрению

Процесс управления изменениями обслуживания сторонними организациями должны учитывать:

a) осуществление изменений в организации:

1) усовершенствование текущих услуг;

2) разработка новых программных приложений и систем;

3) внесение изменений и обновления политики и процедур организации;

4) новые решения для управления инцидентами информационной безопасности и повышения безопасности;

b) осуществление внесения изменений в услуги сторонних организаций:

1) изменения и укрепление к сетям;

2) использование новых технологий;

3) принятие новых продуктов или новых вариантов/версий;

4) развитие новых инструментов и сред;

5) изменения физического расположения обслуживания;

6) смена поставщиков.

10.3 Планирование производительности и загрузки систем

Цель: Свести к минимуму риск сбоев в работе системы.

Для обеспечения доступности данных, требуемой производительности и ресурсов систем необходимо провести предварительное планирование и подготовку.

Для снижения риска перегрузки систем необходимо проводить анализ предполагаемой ее нагрузки.

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

10.3.1 Управление производительностью

Контроль

Необходимо осуществлять прогнозирование, мониторинг и корректировку потребности мощности систем для обеспечения требуемой ее производительности.

Руководство по внедрению

Для обеспечения необходимых мощностей по обработке и хранению информации необходим анализ текущих требований к производительности, а также прогноз будущих. Системы настройки и мониторинга должны быть применены для обеспечения и повышения доступности и эффективности систем. Необходимы меры по управлению для решения проблем в установленные сроки. При прогнозировании должны учитываться новые функциональные и системные требования, а также текущие планы и перспективные планы развития информационных технологий в организации.

Мэйнфреймы требуют особого внимания вследствие значительных финансовых и временных затрат на повышение их производительности. Руководители, отвечающие за предоставление мэйнфреймовых услуг, должны проводить мониторинг загрузки ключевых системных ресурсов. Эти руководители должны определять общие потребности и тенденции в использовании компьютерных ресурсов, что особенно важно для поддержки бизнес-приложений или систем управления для руководства.

Руководители должны использовать эту информацию для идентификации/избежание потенциально узких мест, представляющих угрозу безопасности системы или пользовательским сервисам, а также с целью планирования соответствующих мероприятия по обеспечению информационной безопасности.

10.3.2 Приемка систем

Контроль

Должны быть определены критерии принятия новых и модернизированных информационных систем, новых версий программного обеспечения, а также проведено тестирование систем в процессе их разработки и приемки.

Руководство по внедрению

Требования и критерии для принятия новых систем должны быть четко определены, согласованы, документально оформлены и протестированы.

Новые информационные системы, новые версии и обновления должны быть внедрены в производство только после прохождения официальной приемки. В этих целях необходимо предусмотреть следующие мероприятия по управлению информационной безопасностью:

a) оценка выполнения требований к мощности и производительности компьютеров;

b) определение процедур восстановления после сбоя и повторного запуска, а также формирование планов обеспечения непрерывной работы;

c) подготовка и тестирование типовых операционных процессов на соответствие определенным стандартам;

d) наличие необходимого набора средств контроля информационной безопасности;

e) разработка эффективных руководств по процедурам;

f) обеспечение непрерывности бизнеса в соответствии с требованиями 14.1;

g) обязательная проверка отсутствия неблагоприятного влияния новых систем на существующие, особенно во время максимальных нагрузок, например, в конце месяца;

h) контроль проведения анализа влияния, оказываемого новой системой на общую информационную безопасность организации;

i) организация профессиональной подготовки персонала к эксплуатации и использованию новых систем;

j) легкость в применении, поскольку это затрагивает пользовательскую производительность во избежание ошибок, совершаемых людьми.

Для консультаций на всех этапах разработки новых систем должны привлекаться службы поддержки (эксплуатации) и пользователи с целью обеспечения эффективной эксплуатации проектируемой системы. При этом должны проводиться соответствующие тесты для подтверждения того, что все критерии приемки удовлетворены полностью.

Прочая информация

Приемка может включать в себя официальный процесс освидетельствования и аккредитации для проверки соответствующего соблюдения требований безопасности.

10.4 Защита от вредоносного кода и мобильного кода

Цель: Защищать целостность программного обеспечения и массивов информации.

Необходимо принять меры предотвращения и обнаружения внедрения вредоносного кода и несанкционированного мобильного кода.

Программное обеспечение и средства обработки информации уязвимы к внедрению вредоносного кода, такого как компьютерные вирусы, сетевые «черви», «троянские кони» и логические бомбы. Пользователи должны быть осведомлены об опасности вредоносного кода, а соответствующие руководители должны обеспечить внедрение специальных средств контроля с целью обнаружения и/или предотвращения проникновения вредоносного кода и мобильного кода.

10.4.1 Меры защиты от вредоносного кода

Контроль

Должны быть реализованы меры по обнаружению, предотвращению проникновения и восстановлению после проникновения вредоносного кода, а также должны быть установлены процедуры обеспечения соответствующего оповещения пользователей.

Руководство по внедрению

Защита от вредоносного программного обеспечения должна основываться на понимании требований безопасности, соответствующих мерах контроля доступа к системам и надлежащем управлении изменениями. Необходимо рассматривать следующие мероприятия по управлению информационной безопасностью:

a) документальную политику, требующую соблюдения лицензионных соглашений и устанавливающую запрет на использование неавторизованного программного обеспечения (15.1.2);

b) документированную политику защиты от рисков, связанных с получением файлов и программного обеспечения из внешних сетей, через внешние сети или из любой другой среды. В этой политике должно содержаться указание о необходимости принятия защитных мер;

c) проведение регулярных инвентаризаций программного обеспечения и данных систем, поддерживающих критические бизнес-процессы. Необходима также формализованная процедура по расследованию причин появления любых неавторизованных или измененных файлов в системе;

d) установку и регулярное обновление антивирусного программного обеспечения для обнаружения и сканирования компьютеров и носителей информации, запускаемого в случае необходимости в качестве превентивной меры или рутинной процедуры. Необходимо выполнять следующие проверки:

1) проверку всех файлов на носителях информации сомнительного или неавторизованного происхождения или файлов, полученных из общедоступных сетей, на наличие вирусов перед работой с этими файлами;

2) проверку любых вложений электронной почты и скачиваемой информации на наличие вредоносного программного обеспечения до их использования. Эта проверка может быть выполнена в разных точках, например, на электронной почте, персональных компьютерах или при входе в сеть организации.

3) поверка веб-страниц на наличие вредоносного программного обеспечения;

e) управленческие процедуры и обязанности, связанные с защитой от вирусов, обучение применению этих процедур, а также вопросы оповещения и восстановления после вирусных атак (13.1 и 13.2);

f) соответствующие планы по обеспечению непрерывности бизнеса в части восстановления после вирусных атак, включая все необходимые мероприятия по резервированию и восстановлению данных и программного обеспечения (Раздел 14);

g) внедрение процедур регулярного сбора информации, таких как подписка на почтовые списки и/или проверка веб-сайтов, информирующих о новых вредоносных программных обеспечениях;

h) процедуры по контролю всей информации, касающиеся вредоносного программного обеспечения, обеспечение точности и информативности предупредительных сообщений. Для определения различия между ложными и реальными вирусами должны использоваться профессиональные источники, например, респектабельные журналы, заслуживающие доверия Интернет-сайты или поставщики антивирусного программного обеспечения. Персонал должен быть осведомлен о проблеме ложных вирусов и действиях при их получении.

Прочая информация

Использование двух или нескольких защит программных продуктов от вредоносного кода через среду обработки информации и от различных поставщиков может повысить эффективность защиты от вредоносного кода.

Программное обеспечение для защиты от вредоносного кода должно быть установлено для обеспечения автоматических обновлений файлов, определения и механизмов сканирования, чтобы гарантировать своевременную защиту. Кроме того, программное обеспечение может быть установлено на каждом рабочем компьютере для осуществления автоматических проверок.

При обслуживании и чрезвычайных ситуациях, должны быть приняты меры по защите от внедрения вредоносного кода которые могут идти в обход нормальному контролю защиты от вредоносного кода.

10.4.2 Меры защиты от мобильного кода

Контроль

Там где разрешено использование мобильного кода, конфигурация системы должна обеспечивать уверенность в том, что авторизованный мобильный код функционирует в соответствии с четко определенной политикой безопасности, а исполнение операции с использованием неавторизованного мобильного кода будет предотвращено.

Руководство по внедрению

Для защиты от мобильного кода исполняющего несанкционированные действия необходимо предпринять следующие меры:

a) выполнение мобильного кода в логически изолированной среде;

b) блокирование любого использования мобильного кода;

c) блокирование получения мобильного кода;

d) технические меры должны быть доступными в конкретной системе для обеспечения управления мобильным кодом;

e) контроль над ресурсами, подходящими для мобильного кода доступа;

f) криптографический контроль для уникальной аутентификации мобильного кода.

Прочая информация

Мобильный код является программным кодом, который переводится с одного компьютера на другой, а затем работает автоматически и выполняет конкретную функцию практически без взаимодействия с пользователем. Мобильный код связан с рядом служб промежуточных программных обеспечений.

А также для обеспечения того, чтобы мобильный код не содержал вредоносного кода, необходим контроль за мобильным кодом во избежание несанкционированного использования или сбоя системы, сети и прикладных ресурсов или других нарушений информационной безопасности.

10.5 Резервирование

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

В соответствии с утвержденной стратегией должны устанавливаться регулярные процедуры резервирования (14.1), формирования копий данных и тестирования, их своевременного восстановления.

10.5.1 Резервное копирование

Контроль

Резервные копии информации и программного обеспечения должны создаваться, проверяться и тестироваться на регулярной основе в соответствии с принятыми требованиями резервирования.

Руководство по внедрению

Необходимо обеспечивать адекватные средства резервирования для обеспечения уверенности в том, что важная деловая информация и программное обеспечение смогут быть восстановлены после бедствия или сбоя оборудования. В этих случаях целесообразно применять следующие мероприятия по управлению информационной безопасностью:

a) определить состав информации, подлежащей резервному копированию;

b) выводить точные и полные отчеты по резервным копиям, документировать процедуры копирования и восстановления информации;

c) определить объем резервного копирования (полный или выборочный) и частотность его выполнения должны отражать требования организации, требования безопасности и критичность информации для длительной работы организации;

d) резервные копии во избежание любого повреждения от стихийных бедствий должны храниться в достаточно отдаленном месте от основного здания;

e) резервная информация должны быть обеспечена гарантированным уровнем физической защиты и защиты от воздействий окружающей среды (Раздел 9) в соответствии с уровнем безопасности в основном здании. Мероприятия, применяемые к оборудованию в основном здании, должны распространяться на резервный пункт;

f) резервное оборудование должно регулярно подвергаться тестированию для обеспечения уверенности в том, что в случае возникновения чрезвычайных ситуаций на его работу можно положиться;

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

h) для сохранения конфиденциальности, резервные копии должны быть защищены шифрованием.

Резервное оборудование должны регулярно тестироваться для обеспечения уверенности в том, что они удовлетворяют требованиям планов по обеспечению непрерывности бизнеса (Раздел 14). Необходимо определить соответствующее оборудование для резервного копирования, гарантирующее восстановление всей необходимой информации и программного обеспечения после отказа носителей информации или аварии.

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

Прочая информация

Для упрощения процессов восстановления и резервного копирования информации последовательности операций по резервному копированию могут быть автоматизированы.

Перед реализацией и регулярным выполнением такие автоматизированные решения должны быть в достаточной степени протестированы.

10.6 Управление безопасностью сети

Цель: Обеспечить защиту информации в сетях и защиту поддерживающей инфраструктуры.

Управление безопасностью сетей, которые могут быть расположены за пределами границ организации, требует внимания.

Дополнительные мероприятия по управлению информационной безопасностью могут также потребоваться для защиты важных данных, передаваемых через общедоступные сети.

10.6.1 Средства контроля сети

Контроль

Сети должны быть адекватно управляемыми и контролируемыми в целях защиты от угроз и поддержания безопасности систем и приложений, использующих сеть, включая информацию, передаваемую по сетям.

Руководство по внедрению

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

a) следует распределять ответственность за поддержание сетевых ресурсов и компьютерных операций (10.1.3);

b) следует устанавливать процедуры и обязанности по управлению удаленным оборудованием, включая оборудование, установлено у конечных пользователей;

c) если необходимо, специальные средства контроля следует внедрять для обеспечения конфиденциальности и целостности данных, проходящих по общедоступным или беспроводным сетям, а также для защиты подключенных систем и приложений (11.4 и 12.3). Могут также потребоваться специальные средства контроля для поддержания доступности подключенных сетевых серверов и рабочих станций;

d) следует проводить соответствующую регистрацию и мониторинг для возможной записи безопасности соответствующих действий;

e) действия по управлению необходимо тщательно соизмерять как с требованиями к сервисам от бизнеса, так и с общими требованиями к обеспечению безопасности инфраструктуры обработки информации.

Прочая информация

Дополнительная информация о безопасности сетей содержится в СТ РК ИСО/МЭК 18028-4.

10.6.2 Безопасность сетевых сервисов

Контроль

Меры обеспечения безопасности, уровни обслуживания для всех сетевых услуг и требования управления должны быть определены и включены в любой договор о сетевых услугах независимо от того, предоставляются ли эти услуги своими силами или сторонней организацией.

Руководство по внедрению

Способность поставщика сетевых сервисов для управления согласованных услуг в безопасном режиме должны определяться и регулярно проверяться, и право на проведение аудита должны быть согласованы.

Должны быть определены необходимые меры по безопасности для сетевых услуг, таких как меры обеспечения безопасности, уровни обслуживания и требования управления. Организация должна обеспечить реализацию этих мероприятий поставщиками.

Прочая информация

Сетевые услуги включают предоставление соединений, частные сетевые услуги и сети с дополнительными средствами и управляемыми системами сетевой безопасности, таких как системы сетевой защиты и системы обнаружения вторжений. Эти услуги могут варьироваться от простых неуправляемых пропускной способностью сложных сетей с дополнительными средствами. Мерами обеспечения безопасности сетевых услуг могут быть:

a) технологии применяемые для обеспечения безопасности сетевых услуг, таких как аутентификация, шифрование и контроль сетевых соединений;

b) технические параметры, необходимые для обеспечения соединения с сетью услуг в соответствии с уровнем безопасности и правилами сетевого соединения;

c) процедуры использования сервисной сети для ограничения доступа к сетевым услугам или приложениям, при необходимости.

10.7 Обращение с носителями информации

Цель: Предотвратить несанкционированное разглашение, модификацию, удаление или уничтожение активов и прерывание бизнес-процессов.

Носители информации должны быть проверены и физически защищены.

Должны быть определены соответствующие процедуры защиты документов, компьютерных носителей информации (лент, дисков), данных ввода/вывода и системной документации от повреждения, воровства и неправомочного доступа.

10.7.1 Управление съемными носителями информации

Контроль

Для управления съемными носителями информации должны существовать соответствующие процедуры.

Руководство по внедрению

Для управления съемными носителями информации необходимо рассматривать следующие мероприятия по управлению информационной безопасностью:

a) если носители информации многократного использования больше не требуются и передаются за пределы организации, то их содержимое должно быть уничтожено;

b) носители информации вывозимых за пределы организации должны быть по необходимости авторизованы; о вывозимых носителях должна вестись запись в целях поддержания контрольного учета;

c) все носители информации следует хранить в надежном, безопасном месте в соответствии с требованиями изготовителей;

d) информация, хранимая на носителях и требующая хранения после истечения срока годности (в соответствии с техническими характеристиками), должна храниться в надежном месте во избежании потери информации вследствие износа носителя;

e) при регистрации съемных носителей следует учитывать лимит возможности потери данных;

f) драйверы съемных носителей запускаются только в случае производственной необходимости.

Все процедуры авторизации должны быть четко документированы.

Прочая информация

К съемным носителям относятся магнитные ленты, диски, флэш-диски, съемные жесткие драйверы, компакт-диски, DVD-диски и печатные носители.

10.7.2 Утилизация носителей информации

Контроль

Носители информации, когда в них больше нет необходимости, должны быть надежно и безопасно утилизированы с помощью формализованных процедур.

Руководство по внедрению

Носители информации по окончании использования следует надежно и безопасно утилизировать. Важная информация может попасть в руки посторонних лиц из-за небрежной утилизации носителей данных. Чтобы свести к минимуму такой риск, должны быть установлены формализованные процедуры безопасной утилизации носителей информации. Для этого необходимо предусматривать следующие мероприятия:

a) носители, содержащие важную информацию, следует хранить и утилизировать надежно и безопасно (например, посредством сжигания/измельчения). Если носители информации планируется использовать в пределах организации для других задач, то информация на них должна быть уничтожена;

b) необходимо наличие процедур для идентификации элементов управления по безопасной утилизации;

c) может оказаться проще принимать меры безопасной утилизации в отношении всех носителей информации, чем пытаться сортировать носители по степени важности;

d) многие организации предлагают услуги по сбору и ликвидации документов, оборудования и носителей информации. Следует тщательно выбирать подходящего подрядчика с учетом имеющегося у него опыта и обеспечения необходимого уровня информационной безопасности;

e) по возможности следует регистрировать утилизацию важных объектов с целью последующего аудита.

При накоплении носителей информации, подлежащих утилизации, следует принимать во внимание «эффект накопления», то есть большой объем открытой информации может сделать ее более важной.

Прочая информация

Важная информация может быть скомпрометирована в результате небрежной утилизации носителей информации (см. 9.2.6, информация об утилизации использованного оборудования).

10.7.3 Процедуры обработки информации

Контроль

Для обеспечения защиты информации от несанкционированного раскрытия или неправильного использования необходимо установить процедуры обработки и хранения информации.

Руководство по внедрению

Следует определить процедуры обработки и хранения информации с учетом категорирования информации (7.2). Необходимо использовать следующие мероприятия по управлению информационной безопасностью:

a) обработку и маркирование всех носителей информации, в зависимости от уровня классификации;

b) ограничения доступа с целью идентификации неавторизованного персонала;

c) ограничение формализованной регистрации авторизованных получателей данных;

d) обеспечение уверенности в том, что данные ввода являются полными, процесс обработки завершается должным образом и имеется подтверждение вывода данных;

e) обеспечение защиты информации, находящейся в буфере данных и ожидающей вывода в соответствии с важностью этой информации;

f) хранение носителей информации в соответствии с требованиями изготовителей;

g) сведение рассылки данных к минимуму;

h) четкую маркировку всех копий данных, предлагаемых вниманию авторизованного получателя;

i) регулярный пересмотр списков рассылки и списков авторизованных получателей.

Прочая информация

Эти процедуры должны быть разработаны с учетом категорирования информации, а также в отношении документов, вычислительных систем, сетей, переносных компьютеров, мобильных средств связи, почты, речевой почты, речевой связи вообще, мультимедийных устройств, использования факсов и любых других важных объектов, например, бланков, чеков и счетов.

10.7.4 Безопасность системной документации

Контроль

Системная документация должна быть защищена от несанкционированного доступа.

Руководство по внедрению

С целью защиты системной документации от несанкционированного доступа необходимо применять следующие мероприятия:

a) системную документацию следует хранить безопасным образом;

b) список лиц, имеющих доступ к системной документации, следует сводить к минимуму; доступ должен быть авторизован владельцем бизнес-приложения;

c) системная документация, полученная/поддерживаемая через общедоступную сеть, следует защищать надлежащим образом.

Прочая информация

Системная документация может содержать определенную важную информацию, например, описания процессов работы бизнес-приложений, процедур, структуры данных, процессов авторизации.

10.8 Обмен информацией

Цель: Поддерживать безопасность информации и программного обеспечения при обмене внутри организации и со сторонними организациями.

Обмен информацией и программным обеспечением должен происходить на основе соглашений между организациями и соответствовать действующему законодательству (Раздел 15).

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

10.8.1 Политики и процедуры обмена информацией

Контроль

Должны существовать формализованные процедуры, требования и меры контроля, обеспечивающие защиту обмена информацией при использовании связи всех типов.

Руководство по внедрению

Процедуры и меры контроля должны осуществляться при использовании электронных средств связи для обмена информацией, а также следует рассмотреть следующие пункты:

a) процедуры, предназначенные для защиты обмениваемой информации от прослушивания, копирования, модификации, неправильной маршрутизации и уничтожения;

b) процедуры для обнаружения и защиты от вредоносного кода, который передается путем использования электронных средств связи (10.4.1);

c) процедуры для защиты передаваемой важной электронной информации, выполненной в форме вложенного файла;

d) политика или рекомендации, представляющие приемлемое использование электронных средств связи (см. 7.1.3);

e) процедуры для использования беспроводной связи с учетом существования определенных рисков;

f) сотрудникам, подрядчикам или любым другим работникам запрещается компрометировать организацию, например, путем клеветы, домогательства, лицемерия, пересылки цепных писем («писем счастья»), несанкционированной покупки и т.д.;

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

h) инструкции по сохранению и ликвидации служебной корреспонденции, включая сообщения, согласно соответствующих норм государственных и местных законодательств;

i) не оставлять важную или критическую информацию на печатающих устройствах, например, на копировальных машинах, принтерах, факсимильных аппаратах, так как эта информация может стать доступной для посторонних лиц;

j) контроль и ограничения, связанные с пересылкой средств связи, например, автоматическая пересылка электронной почты на внешние адреса;

k) напоминание сотрудникам о необходимости принятия соответствующих мер предосторожности, например, для исключения подслушивания или перехвата информации при использовании телефонной связи:

1) лицами, находящимися в непосредственной близости, особенно при пользовании мобильными телефонами;

2) прослушивания телефонных переговоров путем физического доступа к трубке, телефонной линии или с использованием сканирующих приемников при применении аналоговых мобильных телефонов;

3) посторонними лицами со стороны адресата:

l) не оставлять сообщений на автоответчиках, переадресация на которые произошла вследствие ошибки соединения, или автоответчиках операторов связи, поскольку эти сообщения могут быть воспроизведены неавторизованными лицами;

m) напоминание сотрудникам о возможных рисках, присущих факсимильных аппаратов, а именно:

1) несанкционированный доступ к встроенным памяти для поиска сообщений;

2) преднамеренное или случайное программирование аппаратов с целью передачи сообщений по определенным номерам;

3) отсылка документов и сообщений по неправильному номеру вследствие неправильного набора либо из-за использования неправильно сохраненного номера:

n) напоминание персоналу о не допустимости регистрации статистических данных, такие как адреса электронной почты или другой личной информации, в программном обеспечении, чтобы избежать несанкционированных действий;

o) напоминание сотрудникам о том, что современные факсимильные аппараты, фотокопировальные устройства снабжены кэш-страницами, и сохраняют страницы в случае дефекта бумаги или передачи, которые после устранения ошибки будут пропечатываться еще один раз. Кроме того, сотрудникам следует напомнить о том, что не следует вести конфиденциальные беседы в общественных местах, открытых офисах и в переговорных комнатах с тонкими стенами.

Обмен информацией должен быть под контролем и соответствовать действующему законодательству (Раздел 15).

Прочая информация

Обмен информацией может происходить с использованием ряда различных средств связи, включая электронную и речевую связь, факсимильную и видеосвязь.

Обмен программными обеспечениями может происходить с использованием ряда различных носителей, включая скачивание из сети Интернет или приобретения у поставщиков, предоставляющих готовую продукцию.

Следует рассматривать служебные, правовые и защитные последствия, связанные с обменом электронных данных, услугами электронной торговли и электронными коммуникациями, а также требования по управлению информационной безопасностью.

Информация может быть перехвачена при обмене информацией, нарушение политики и процедур использования средств связи, например, подслушивание при использовании мобильных телефонов в общественном месте, неправильных сообщений по электронной почте, прослушивание автоответчика, несанкционированного доступа к системам речевой связи или неправильной передачи сообщений на факсимильном аппарате.

Из-за перехвата информации могут быть нарушены бизнес-операции, а также при сбоях средств связи, их перегрузки или прерывания (10.3 и Раздел 14). Информация может быть под угрозой при доступе неавторизованных пользователей (Раздел 11).

10.8.2 Соглашения по обмену информацией

Контроль

Между организацией и сторонними организациями должны быть заключены соглашения по обмену информацией и программным обеспечением.

Руководство по внедрению

Необходимо, чтобы требования безопасности в подобных соглашениях учитывали:

a) обязанности руководства по контролю и уведомлению о передаче, отправке и получении информации;

b) процедуры для уведомления отправителя о передаче, отправке и получении информации;

c) процедуры для обеспечения прослеживаемости и строгого выполнения обязательств;

d) минимальные технические требования по формированию и передаче пакетов данных;

e) соглашения об условном депонировании;

f) требования к курьерской службе;

g) ответственности и обязательства в случае потери данных;

h) применение согласованной системы маркировки для важной или критичной информации, обеспечивающей уверенность в том, что значение этой маркировки будет сразу же понятно и информация будет соответственно защищена;

i) определение владельцев информации и программного обеспечения, а также обязанностей по защите данных, учет авторских прав на программное обеспечение и аналогичных вопросов (см. 15.1.2 и 15.1.4);

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

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

Политики, процедуры и стандарты безопасности должны быть внедрены и поддержаны для защиты физических носителей информации при транспортировке (см. 10.8.3) и рассмотрены в соглашениях по обмену информацией.

В соглашениях необходимо отразить безопасность и важность вовлеченной служебной информации.

Прочая информация

Соглашения могут быть выполнены как электронным способом, так и вручную и принимать форму официального контракта или условий трудового договора. Для важной

информации, конкретные механизмы, используемые для целей обмена такой информации должны быть общими для всех организаций в виде соглашений.

10.8.3 Защита физических носителей информации при транспортировке

Контроль

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

Руководство по внедрению

Для защиты информации во время их транспортировки между организациями, необходимо применять следующие меры:

a) следует использовать надежных перевозчиков или курьеров;

b) список авторизованных курьеров необходимо согласовывать с руководством;

c) следует внедрить процедуры проверки идентификации курьеров;

d) упаковка должна быть достаточной для защиты содержимого от любого физического повреждения, которое может иметь место при транспортировке, и соответствовать требованиям изготовителей носителей информации (например, программного обеспечения), защиту от каких-либо факторов окружающей среды, сокращающих эффективность восстановления носителя информации, таких как воздействие высокой температуры, влажности или электромагнитного поля;

e) специальные средства контроля следует применять, при необходимости, для защиты важной информации от неавторизованного раскрытия или модификации. Например:

1) использование запертых контейнеров;

2) личную доставку;

3) использование упаковки, которую нельзя нарушить незаметно (на которой видна любая попытка вскрытия);

4) в исключительных случаях, разбивку отправления на несколько частей, пересылаемых различными маршрутами.

Прочая информация

Информация может быть искажена или скомпрометирована вследствие несанкционированного 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

Контроль

Информация, используемая в электронном обмене сообщениями, должна быть защищена надлежащим образом.

Руководство по внедрению

Вопросы безопасности электронных сообщений должна включать в себя следующее:

a) уязвимость сообщений по отношению к возможности от несанкционированного доступа или модификации, а также к отказу в обслуживании;

b) обеспечение правильных решений и транспортировки сообщений;

c) общую надежность и доступность данной услуги;

d) правовые вопросы, например, требования в отношении электронных подписей;

e) получить предварительное согласие на использование внешних общественных услуг, таких как мгновенные файлы сообщения или совместное использование файлов;

f) надежные уровни аутентификации контроля доступа к общедоступным сетям.

Прочая информация

Электронные обмены сообщениями такие как электронная почта, электронный обмен данными (ЭОД) и мгновенные сообщения играют более важную роль в бизнес-

коммуникации. Электронные сообщения более подвержены риску по сравнению с бумажными системами связи.

10.8.5 Системы бизнес-информации

Контроль

Требования и процедуры должны быть разработаны и внедрены для защиты информации, связанной с взаимодействием систем бизнес-информации.

Руководство по внедрению

Рассмотрение безопасности и бизнес-последствий таких взаимосвязанных объектов должны включать:

a) известные уязвимости в административной системе и системе учета, где информацией пользуются между разными подразделениями организации;

b) уязвимость информации в офисных системах, связана, например с записью телефонных разговоров или переговоров по конференц-связи, конфиденциальностью звонков, хранением факсов, вскрытием и рассылкой почты;

c) требования и соответствующие средства контроля для совместного использования информации;

d) исключение использования офисных систем в отношении категорий важной служебной информации, если эти системы не обеспечивают соответствующий уровень защиты (7.2);

e) уязвимость доступа к данным личных ежедневников отдельных сотрудников, например, работающих на важных проектах;

f) категории сотрудников, подрядчиков или бизнес-партнеров позволило бы использовать систему и местоположение, с которых может осуществляться доступ (6.2 и 6.3);

g) ограничение определенных возможностей системы для определенных категорий пользователей;

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

i) сохранение и резервирование информации, содержащейся в системе (10.5.1);

j) требования системы восстановления и размещения (Раздел 14).

Прочая информация

Электронные офисные системы обеспечивают возможность для быстрого распространения и совместного использования служебной информации путем использования сочетания возможностей документов, компьютеров, переносных компьютеров, мобильных средств связи, почты, электронной почты, речевой связи вообще, мультимедийных систем, сервисов доставки почтовых отправлений и факсов.

10.9 Услуги электронной торговли

Цель: Обеспечить безопасность услуг электронной торговли и их безопасное использование.

Необходимо учесть последствия безопасности, связанные с использованием услуг электронной торговли и транзакции в режиме реального времени (on-line), а также организационных мероприятий по управлению информационной безопасностью. Следует принимать во внимание целостность и доступность информации проходящую по общедоступным сетям.

10.9.1 Электронная торговля

Контроль

Информация, используемая в электронной торговле, проходящая по общедоступным сетям, должна быть защищена от мошенничества, оспаривания контрактов, а также от несанкционированного разглашения и модификации.

Руководство по внедрению

Для обеспечения безопасности электронной торговли, необходимы:

a) аутентификация. С какой степенью клиенту и продавцу следует проверять идентификацию друг друга;

b) авторизация. Кто уполномочен устанавливать цены, подготавливать или подписывать ключевые коммерческие документы;

c) каким образом об авторизации может быть проинформирован торговый партнер.

d) процессы в отношении контрактов и тендеров. Какие требования существуют в отношении конфиденциальности, целостности, подтверждения отправки и получения ключевых документов, а также в невозможности отказа от совершенных сделок;

e) информация о ценах. На сколько можно доверять рекламе прайс-листов. конфиденциальности в отношении существенных сделок;

f) конфиденциальность в отношении существенных сделок;

g) обработка заказов. Как обеспечиваются конфиденциальность и целостность деталей заказа, условий оплаты и адреса доставки, а также подтверждение при его получении;

h) контрольные проверки. Какая степень контроля является достаточной, чтобы проверить информацию об оплате, предоставленную клиентом;

i) расчеты. Какая форма оплаты является наиболее защищенной от мошенничества;

j) оформление заказов. Какая требуется защита, чтобы обеспечить конфиденциальность и целостность информации о заказах;

k) предотвращение потери или дублировании сделок;

l) ответственность за риск любых мошеннических сделок;

m) требования страхования.

Многие из вышеупомянутых проблем могут быть решены с использованием криптографических методов в соответствии с 12.3, при этом необходимо обеспечить соответствие требованиям законодательства (15.1, 15.1.6 относительно законодательства в области криптозащиты).

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

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

Необходимо обеспечивать устойчивость к вирусным атакам в процессе проведения электронной торговли, а также предусматривать последствия безопасности всех сетевых взаимосвязей при ее осуществлении (11.4.6).

Прочая информация

Электронная торговля подвержена ряду сетевых угроз, которые могут привести к краже, оспариванию контрактов, а также раскрытию или модификации информации.

Услугами электронной торговли, для уменьшения рисков, могут использоваться надежные методы аутентификации, например, использования криптографических ключей и цифровых подписей (см. 12.3), а также услугами могут воспользоваться доверенные лица сторонних организаций.

10.9.2 Транзакции в режиме реального времени (on-line)

Контроль

Информация, используемая в транзакциях в режиме реального времени (on-line), должна быть защищена для предотвращения неполной передачи, неправильной маршрутизации, несанкционированного изменения сообщений, несанкционированного

разглашения, несанкционированного копирования или повторного воспроизведения сообщений.

Руководство по внедрению

Из соображений безопасности для онлайновой транзакции должно быть включено следующее:

a) использование электронных подписей каждой стороной, участвующей в транзакции;

b) все аспекты транзакции, т.е. обеспечение того, что:

1) учетные данные всех сторон, являются действительными и проверены;

2) транзакция остается конфиденциальной;

3) сохраняется конфиденциальность, связанная со всеми заинтересованными сторонами;

c) линии связи между всеми заинтересованными сторонами должны быть зашифрованы;

d) обеспечение протоколами, используемыми для обмена данными между всеми заинтересованными сторонами;

e) обеспечение хранения подробности транзакции расположенного вне какой-либо общедоступной среды, например, на платформе хранения данных, существующих в корпоративной сети Интранет, а также не сохранятется и выставляется на носителе хранения данных, прямо доступных из сети Интернет;

f) в случае использования доверия (например, в целях выдачи и сохранения цифровых подписей и/или цифровых сертификатов) необходимо объединять меры по обеспечению безопасности и внедрять в течение всего непрерывного процесса управления сертификатом/подписью.

Прочая информация

Принятые меры управления необходимо соизмерять с уровнем риска, связанных с каждой формой он-лайн транзакции.

Транзакции должны соответствовать законам, правилам и нормам, установленным в юрисдикции, в которой транзакция производится, обрабатывается, завершается и/или хранится.

Существуют различные формы транзакции, которые могут быть выполнены сетевым способом, например, договорные, финансовые и т.д.

10.9.3 Общедоступная информация

Контроль

Информация, предоставляемая через общедоступную систему, должна быть защищена от несанкционированной модификации.

Руководство по внедрению

Программное обеспечение, данные и другую информацию, требующую высокого уровня целостности, доступ к которой осуществляется через системы публичного доступа необходимо защищать адекватными способами, например, посредством цифровой подписи (12.3).

Необходим соответствующий формализованный процесс авторизации прежде, чем информация будет общедоступной. Кроме того, все входящие данные, предоставленные в систему со стороны должны быть проверены и одобрены.

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

a) полученная информация соответствовала всем законам по защите данных (15.1.4);

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

c) важная информация была защищена в процессе ее сбора и хранения;

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

Прочая информация

Информацию системы публичного доступа, например, информацию на Web-сайте, доступную через Интернет, возможно, потребуется привести в соответствие с законодательством и регулирующими нормами страны, под юрисдикцией которых находится система или осуществляется торговля.

Несанкционированная модификация опубликованной информации может нанести ущерб репутации издательской организации.

10.10 Мониторинг

Цель: Обнаружение несанкционированных действий по обработке информации.

Системы должны контролироваться и события информационной безопасности должны быть зарегистрированы. Оператор журнала регистрации и ошибок должен быть использован и определен для обеспечения информационных задач системы.

Организация должна соблюдать все соответствующие правовые требования, предъявляемые к мониторингу и регистрации событий.

Мониторинг системы позволяет проверять эффективность применяемых мероприятий по обеспечению информационной безопасности и подтверждать соответствие модели политики доступа требованиям бизнеса.

10.10.1 Ведение журналов аудита

Контроль

Должны быть обеспечены ведение и хранение в течение определенного периода времени журналов аудита, регистрирующих действия пользователей, нештатные ситуации и события информационной безопасности, в целях помощи в будущих расследованиях и проведении мониторинга контроля доступа.

Руководство по внедрению

В журналы аудита должны быть включены:

a) ID пользователи;

b) даты и время входа и выхода;

c) идентификатор терминала и его местоположение, если возможно;

d) записи успешных и отклоненных попыток доступа к системе;

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

f) изменение конфигурации системы;

g) использование привилегий;

h) использование системных утилит и приложений;

i) доступ к файлам и типы доступа;

j) сетевые адреса и протоколы;

k) тревожные сигналы, подаваемые системой контроля доступа;

l) активации и деактивации систем защиты, таких как антивирусные системы и системы обнаружения вторжений.

Прочая информация

В журналах аудита могут содержаться навязчивые личные и конфиденциальные данные. Должны быть приняты соответствующие меры защиты конфиденциальности (см. также 15.1.4). При возможности, системные администраторы не должны иметь разрешение на удаление или деактивацию журналов регистрации их собственных действий (см. 10.1.3).

10.10.2 Мониторинг использования средств обработки информации

Контроль

Должны быть установлены процедуры, позволяющие вести мониторинг и регулярный анализ результатов мониторинга использования средств обработки информации.

Руководство по внедрению

Уровень мониторинга конкретных средств обработки информации следует определять на основе оценки рисков. Организация должна соблюдать все соответствующие законодательные требования, применяемые к мониторинговой деятельности. При мониторинге следует обращать внимание на:

a) авторизованный доступ, включая следующие детали:

1) пользовательский ID;

2) дату и время основных событий;

3) тип событий;

4) файлы, к которым был осуществлен доступ;

5) используемые программы/утилиты;

b) все привилегированные действия, такие как:

1) использование учетной записи супервизора;

2) запуск и остановка системы;

3) подсоединение/отсоединение устройства ввода/вывода;

c) попытки несанкционированного доступа, такие как:

1) неудавшиеся или отклоненные попытки пользователя;

2) неудавшиеся или отклоненные попытки доступа к данным и другим ресурсам;

3) нарушение политики доступа и уведомления сетевых шлюзов и систем сетевой защиты;

4) предупреждения от собственных систем обнаружения вторжений;

d) предупреждения или отказы системы, такие как:

1) консольные (терминальные) предупреждения или сообщения;

2) исключения, записанные в системные журналы регистрации;

3) предупредительные сигналы, связанные с управлением сетью;

4) оповещения, созданные системой управления доступом;

e) изменения или попытки изменения настроек безопасности системы и средств управления.

Частота рассмотрения результатов мониторинга должна определяться вовлеченными рисками. Должны быть рассмотрены факторы риска, в том числе:

a) критичность процессов приложений;

b) значимость, важность и критичность вовлеченной информации;

c) прошлый опыт несанкционированного проникновения в систему и ее неправильного использования, частота использования уязвимых мест;

d) степень взаимосвязи информационных систем организации с другими (особенно общедоступными) сетями;

e) регистрация деактивации средства.

Прочая информация

Необходимо определить процедуры мониторинга использования средств обработки информации для обеспечения уверенности в том, что пользователи выполняют только те действия, на которые они были явно авторизованы.

Анализ (просмотр) журнала аудита подразумевает понимание угроз, которым подвержена система, и причин их возникновения. Примеры событий, которые могли бы потребовать дальнейшего исследования в случае инцидентов нарушения информационной безопасности, приведены в 13.1.1.

10.10.3 Защита информации журналов регистрации

Контроль

Средства регистрации и информация журналов регистрации должны быть защищены от вмешательства и несанкционированного доступа.

Руководство по внедрению

Средства управления должны обеспечить защиту от внесения несанкционированных изменений в отчеты и препятствованию работы оборудования создания отчетов, в том числе:

a) изменение типов зарегистрированных сообщений;

b) редактирование или удаление файлов отчетов;

c) превышения вместимости носителей информации, на которых хранятся отчеты, в результате чего происходят сбои записи событий или перезапись последних зарегистрированных событий.

Некоторые отчеты аудита нуждаются в архивации в соответствии с правилами сохранения записей отчетов, либо для выполнения требований по сбору и сохранению подтверждающей информации (13.2.3).

Прочая информация

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

Системные журналы отчетов должны быть защищены, так как при изменении или удалении данных в них, существующие отчеты могут создавать ложное впечатление о безопасности.

10.10.4 Журналы регистрации действий администратора и оператора

Контроль

Деятельность системного администратора и системного оператора должны быть регистрируемыми.

Руководство по внедрению

Отчеты должны содержать:

a) время, в которое произошло событие (успешное или неуспешное завершение операции);

b) информация о событии (например, обработанные файлы) или о сбое (например, произошла ошибка, и были предприняты корректирующие действия);

c) сведения о том, какая использовалась учетная запись и какой администратор или оператор выполнял соответствующие операции;

d) сведения о том, какие использовались процессы.

Журналы регистрации действий системного администратора и оператора должны подлежать пересмотру на регулярной основе.

Прочая информация

Необходимо предусмотреть систему мониторинга корректности операций, выполняемых администраторами системы и сети, в которой может использоваться система обнаружения вторжений, управляемая за пределами системы.

10.10.5 Регистрация неисправностей

Контроль

Неисправности должны быть зарегистрированы, проанализированы и устранены.

Руководство по внедрению

Необходимо регистрировать сообщения пользователей о неисправностях, связанных с обработкой информации или системами связи. Должны существовать четкие правила обработки допущенных неисправностей, включающие:

a) анализ неисправностей для обеспечения уверенности в том, что они были удовлетворительным образом устранены;

b) анализ предпринятых корректирующих мер, обеспечивающих уверенность в том, что мероприятия по управлению информационной безопасностью не были скомпрометированы (нарушены) и предпринятые действия надлежащим образом авторизованы.

Необходимо убедиться, что регистрация ошибок приводится в действие, если системная функция доступна.

Прочая информация

Регистрация ошибок и неисправностей может воздействовать на работу системы. Такая регистрация должна проводиться компетентным персоналом, и уровень регистрации необходимого для индивидуальной системы, должны определяться оценкой степени риска с учетом ухудшения работы.

10.10.6 Синхронизация часов

Контроль

Часы всех соответствующих систем обработки информации в пределах организации или охраняемой зоны должны быть синхронизированы с помощью единого источника точного времени.

Руководство по внедрению

Там где компьютер или устройство связи имеют возможность использовать часы в реальном времени, их следует устанавливать по Универсальному Скоординированному Времени (UTC) или местному стандартному времени. Так как некоторые часы, как известно, «уходят вперед» или «отстают», должна существовать отдельная процедура, которая проверяет и исправляет любое отклонение или его значимое изменение.

Для обеспечения соответствия записей времени реальным датам и времени важна правильная интерпретация формата даты и времени. Следует принять во внимание местные специальные часы (например, переход на летнее время).

Прочая информация

Правильная установка компьютерных часов (таймера) важна для обеспечения точности заполнения журналов аудита, которые могут потребоваться для расследований или как доказательство при судебных или и административных разбирательствах. Некорректные журналы аудита могут затруднять такие расследования, а также приводить к сомнению в достоверности собранных доказательств. В качестве основных часов для систем регистрации могут использоваться часы, связанные с сигналами точного времени, передаваемыми через радиовещательную сеть, которые в свою очередь, привязаны к показаниям национальных стандартных атомных часов. Для поддержания синхронности всех серверов с основными часами может использоваться сетевой протокол установки времени.

11 Контроль доступа

11.1 Бизнес-требования к контролю доступа

Цель: Контролировать доступ к информации.

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

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

11.1.1 Политика контроля доступа

Контроль

Политика контроля доступа должна быть установлена и документирована с учетом потребности бизнеса и безопасности информации.

Руководство по внедрению

Правила контроля доступа и права каждого пользователя или группы пользователей должны быть однозначно определяться политикой безопасности. Контроль доступом может быть логическим и физическим (см. Раздел 9) и их необходимо рассматривать вместе. Пользователи и поставщики услуг должны быть оповещены о необходимости и выполнения требований в отношении логического доступа.

Необходимо, чтобы в политике было учтено следующее:

a) требования безопасности конкретных бизнес-приложений;

b) идентификация всей информации, связанной с функционированием бизнес-приложений;

c) условия распространения информации и авторизации доступа, например, применение принципа «need to know» (пользователь получает доступ только к данным, безусловно необходимым ему для выполнения конкретной функции), а также в отношении категорированной информации и требуемых уровней ее защиты (7.2);

d) согласованность между политиками по контролю доступа и классификации информации применительно к различным системам и сетям;

e) применяемое законодательство и любые договорные обязательства относительно защиты доступа к данным или сервисам (15.1);

f) стандартные профили доступа пользователя для типовых обязанностей и функций;

g) управление правами доступа в распределенной сети с учетом всех типов доступных соединений;

h) распределение обязанностей к контролю доступа, например, право доступа, авторизация доступа, администрирование доступа;

i) требования формализованной авторизации прав доступа (11.2.1);

j) требования периодического пересмотра прав доступа (11.2.4);

k) аннулирование прав доступа (8.3.3).

Прочая информация

При определении правил контроля доступа следует принимать во внимание следующее:

a) дифференциацию между правилами, обязательными для исполнения, и правилами, которые являются общими или применяемыми при определенных условиях;

b) установление правил, основанных на предпосылке «все должно быть в общем случае запрещено, пока явно не разрешено», а не на более слабом принципе «все в общем случае разрешено, пока явно не запрещено»;

c) изменения в признаках маркировки информации (7.2), как генерируемых автоматически средствами и обработки информации, так и инициируемых по усмотрению пользователей;

d) изменения в правах пользователя как устанавливаемых автоматически информационной системой, так и определенных администратором;

e) правила, которые требуют одобрения администратора или другого лица перед применением, а также те, которые не требуют специального одобрения.

Правила контроля доступом должны быть поддержаны формализованными процедурами и четко определенными обязанностями (6.1.3, 11.3, 10.4.1, 11.6).

11.2 Управление доступом пользователей

Цель: Предотвратить несанкционированный доступ пользователей к

информационным системам и обеспечить авторизованный доступ пользователей к этим системам.

Для контроля за предоставление права доступа к информационным системам и сервисам необходимо наличие формализованных процедур.

Процедуры должны охватывать все стадии жизненного цикла пользовательского доступа от начальной регистрации новых пользователей до конечного снятия с регистрации пользователей, которым больше не требуется доступ к информационным системам и сервисам. Особое внимание следует уделять мероприятиям в отношении предоставления прав привилегированного доступа, с помощью которых пользователи могут обходить системные средства контроля.

11.2.1 Регистрация пользователей

Контроль

Необходимо существование формализованной процедуры регистрации и снятия с регистрации пользователей в отношении предоставления доступа ко всем многопользовательским информационным системам и сервисам.

Руководство по внедрению

Доступ к многопользовательским информационным сервисам должен быть контролируемым посредством формализованного процесса регистрации пользователей, который должен включать:

a) использование уникальных ID (идентификатор или имен) пользователей, таким образом, чтобы действия в системе можно было бы соотнести с пользователями и установить ответственных. Использование групповых ID следует разрешать только в тех случаях, где это необходимо с учетом особенностей выполняемой работы;

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

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

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

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

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

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

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

i) периодическую проверку и удаление избыточных пользовательских ID и учетных записей (11.2.4);

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

Прочая информация

Следует рассмотреть вопрос о создании обязанностей в отношении доступа пользователя на основе требований бизнеса, которые необходимо обобщить ряд прав доступа в типичные профили доступа пользователей (11.2.4). Пересмотр прав доступа

пользователей управляются на уровне таких обязанностей легче чем на уровне отдельных прав.

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

11.2.2 Управление привилегиями

Контроль

Предоставление и использование привилегий должно быть ограниченным и контролируемым.

Руководство по внедрению

Необходимо, чтобы в многопользовательских системах, которые требуют защиты от неавторизованного доступа, предоставление привилегий контролировать посредством формализованного процесса авторизации.

При этом целесообразно применять следующие меры:

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

b) привилегии должны предоставляться только тем сотрудникам, которым это необходимо для работы и только на время ее выполнения (11.1.1), например, предоставляя минимальные возможности по работе с системой для выполнения требуемых функций, только когда в этом возникает потребность;

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

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

e) проводить политику разработки и использования программ, которые позволяют избежать необходимости работать с привилегиями следует поощрять;

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

Прочая информация

Предоставление и использование привилегий при применении средств многопользовательской информационной системы, которые позволяют пользователю обходить средства контроля системы или бизнес приложения, необходимо ограничивать и держать под контролем. Неадекватное использование привилегий часто бывает главной причиной сбоев систем.

11.2.3 Управление паролями пользователей

Контроль

Предоставление паролей должно контролироваться посредством формализованного процесса управления.

Руководство по внедрению

Процесс управления должен включать следующие требования:

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

b) в случаях, когда от пользователей требуется управление собственными паролями, необходимо обеспечивать предоставление безопасного первоначального временного

пароля (11.3.1), который пользователя принуждают сменить при первой регистрации в системе;

c) установить процедуры, чтобы проверить идентичность пользователя до обеспечения нового, замены или временного пароля;

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

e) временные пароли должны быть индивидуальными и не подвержены легкому угадыванию;

f) пользователям необходимо подтверждать получение паролей;

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

h) заданные по умолчанию пароли поставщиков должны быть измененными после установки системы или программного обеспечения.

Прочая информация

Пароли являются наиболее распространенными средствами подтверждения идентификатора пользователя при доступе к информационной системе или сервису. При необходимости следует рассматривать возможности других технологий для идентификации и аутентификации пользователя, такие как биометрия (проверка отпечатков пальцев), проверка подписи, использование аппаратных средств идентификации (чип-карт, микросхем).

11.2.4 Пересмотр прав доступа пользователей

Контроль

Руководство периодически должно осуществлять формализованный процесс пересмотра прав доступа пользователей.

Руководство по внедрению

Для пересмотра прав доступа необходимы следующие мероприятия:

a) права доступа пользователей должны пересматриваться регулярно (рекомендуемый период – 6 месяцев) и после любых изменений, таких как продвижение по службе, понижение или увольнение с работы (11.2.1);

b) права доступа пользователей должны подлежать пересмотру и перераспределяться при переходе с одной работы на другую внутри организации;

c) авторизация специальных привилегированных прав доступа (11.2.2) должна осуществляться через меньшие интервалы времени (рекомендуемый период – 3 месяца);

d) предоставление привилегии должны периодически проверяться для обеспечения уверенности в том, что не были получены неавторизованные привилегии;

e) изменения к привилегированным учетным записям должны быть зарегистрированы для периодического пересмотра.

Прочая информация

Необходимо проводить регулярный пересмотр прав доступа пользователей для поддержания эффективного контроля доступа к данным информационным услугам.

11.3 Ответственность пользователей

Цель: Предотвращать несанкционированный доступ пользователей, а также компрометацию или кражу информации и средств обработки информации.

Взаимодействие авторизованных пользователей является важным аспектом эффективности безопасности.

Пользователи должны быть осведомлены о своих обязанностях по использованию эффективных мероприятий по управлению доступом, в частности, в отношении паролей и безопасности оборудования, с которым они работают. Политика чистого стола и чистого

экрана должна реализовываться для снижения рисков неавторизованного доступа или повреждения документов, носителей и средств обработки информации.

11.3.1 Использование паролей

Контроль

Пользователи должны соблюдать определенные правила обеспечения безопасности при выборе и использовании паролей.

Руководство по внедрению

Все пользователи должны быть осведомлены о необходимости:

a) сохранения конфиденциальности паролей;

b) запрещения записи паролей на бумаге, на файле программного обеспечения или на переносных устройствах, если только не обеспечено безопасное их хранение;

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

d) выбора качественных паролей с минимальной длиной, которые:

1) легко запомнить;

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

3) не уязвимы для атаки по словарю (т.е. не состоят из слов, включенных в словари);

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

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

f) изменения временных паролей при первой регистрации в системе;

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

h) исключения коллективного использования индивидуальных паролей;

i) не использовать один и тот же пароль для коммерческих и некоммерческих целей.

Если пользователи нуждаются в доступе к многочисленным услугам или бизнес-приложениям и вынуждены использовать многочисленные пароли, можно порекомендовать возможность использования одного качественного пароля (11.3.1,d) для всех сервисов, обеспечивающих разумный уровень защиты хранимого пароля.

Прочая информация

Управление системой компьютерной службы помощи, контакт с потерянными или забытыми паролями, нуждаются в особом внимании, поскольку это может также быть средством атаки к системе пароля.

11.3.2 Оборудование, оставленное пользователем без присмотра

Контроль

Пользователи должны обеспечивать соответствующую защиту оборудования, оставленного без присмотра.

Руководство по внедрению

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

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

b) отключаться от мэйнфрейма, когда сеанс закончен (то есть не только выключать PC или терминал);

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

Прочая информация

Оборудование, установленное в рабочих зонах, например рабочие или файловые станции, требует специальной защиты от неавторизованного доступа в случае оставления их без присмотра на длительный период.

11.3.3 Политика «чистого стола» и «чистого экрана»

Контроль

Организациям следует применять политику «чистого стола» в отношении бумажных документов и сменных носителей данных, а также политику «чистого экрана» в отношении средств обработки информации.

Руководство по внедрению

Политика чистого стола и чистого экрана должна учитывать категории информации с точки зрения безопасности (7.2), законодательные требования и договорные обязательства (15.1), и соответствующие риски, а также корпоративную культуру организации. Необходимо учитывать следующие мероприятия:

a) носители с важной или критичной служебной информацией, когда они не требуются, следует убирать и запирать (например, в несгораемом сейфе или шкафу), особенно когда помещение пустует;

b) персональные компьютеры, компьютерные терминалы и принтеры должны быть выключены по окончании работы; следует также применять кодовые замки, пароли или другие мероприятия в отношении устройств, находящихся без присмотра;

c) необходимо обеспечить защиту пунктов отправки/приема корреспонденции, а также факсимильных и телексных аппаратов в случаях нахождения их без присмотра;

d) в нерабочее время фотокопировальные устройства следует запирать на ключ (или защищать от неавторизованного использования другим способом);

e) напечатанные документы с важной или конфиденциальной информацией необходимо изымать из принтеров немедленно.

Прочая информация

Политика «чистого стола» и «чистого экрана» сокращает риски неавторизованного доступа, потери или повреждения информации как во время рабочего дня, так и при внеурочной работе. Если носители информации заперты в несгораемых сейфах, шкафах или в других безопасных местах хранения, то могут быть сохранены при бедствии, например, при пожаре, землетрясении, наводнении или взрыве.

Рекомендуется использовать принтер с кодовой функцией для получения пользователем напечатанных документов, находясь рядом с принтером.

11.4 Контроль сетевого доступа

Цель: защита сетевых сервисов.

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

Это необходимо для уверенности в том, что пользователи, которые имеют доступ к сетям и сетевым сервисам, не компрометируют их безопасность, обеспечивая:

a) соответствующие интерфейсы между сетью организации и сетями, принадлежащими другим организациям, или общедоступными сетями;

b) соответствующие механизмы аутентификации в отношении пользователей и оборудования;

c) контроль доступа пользователей к информационным сервисам.

11.4.1 Политика в отношении использования сетевых услуг

Контроль

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

Руководство по внедрению

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

a) сети и сетевые услуги, к которым разрешен доступ;

b) процедуры авторизации для определения кому, к каким сетям и сетевым сервисам разрешен доступ;

c) мероприятия и процедуры по защите от несанкционированного подключения к сетевым сервисам;

d) средства, используемые для доступа к сетям и сетевым сервисам (например, условия для того, чтобы позволить доступ по телефонной связи поставщику услуг сети Интернет или отдаленной системе).

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

Прочая информация

Несанкционированные и незащищенные подключения к сетевыми службам могут нарушать информационную безопасность целей организации. Контроль доступа, в частности, является необходимым для сетевых подключений к важным или критичным бизнес-приложениям или для пользователей, находящихся в зонах высокого риска, например, в общественных местах или за пределами организации – вне сферы непосредственного управления и контроля безопасности со стороны организации.

11.4.2 Аутентификация пользователей для внешних соединений

Контроль

Для контроля доступа удаленных пользователей должны быть применены соответствующие методы аутентификации.

Руководство по внедрению

Аутентификация удаленных пользователей может быть достигнута при использовании средств криптографии, средств идентификации аппаратуры или протоколов, поддерживающих метод «отклик-отзыв». Возможные пути реализации таких средств можно найти в различных решениях виртуальных частных сетях (VPN). Выделенные частные линии пользователя могут также использоваться для обеспечения доверия к источнику подключений.

Процедуры и средства контроля обратного вызова, например, использование модемов с обратным вызовом, могут обеспечивать защиту от неавторизованных и нежелательных подключений к средствам обработки информации организации, так как подтверждает право на доступ пользователей, пытающихся установить удаленную связь с сетью организации. При использовании этих способов организации не следует использовать сетевые сервисы, которые включают переадресацию вызова. Если же они используются, необходимо блокировать возможности переадресации, чтобы избежать связанных с этим рисков.

Процесс обратного вызова должен обеспечивать уверенность в том, что фактическое разъединение на стороне организации осуществлено. В противном случае удаленный пользователь может держать линию занятой, фальсифицируя проверку обратного вызова. Для исключения подобных инцидентов процедуры и средства контроля обратного вызова следует тщательно тестировать.

Аутентификация узла может служить альтернативным средством аутентификации групп удаленных пользователей там, где они подсоединены к безопасному компьютерному средству совместного использования. Криптографические методы, например, основанные на паспорте оборудования, могут быть использованы для аутентификации узлов. Это является частью нескольких VPN решений.

Дополнительный контроль аутентификации должен быть выполнен для контроля доступа к беспроводным сетям. В частности, особое внимание необходимо в выборе мер контроля для беспроводных сетей в связи с большими незамеченными перехватами и включениями нагрузки сети связи.

Прочая информация

Внешние соединения обеспечивают потенциал для неавторизованного доступа к служебной информации, например, при использовании телефонной связи. Поэтому, при доступе удаленных пользователей, они должны быть аутентифицированы. Некоторые методы аутентификации обеспечивают больший уровень защиты, например, основанные на использовании средств криптографии, и могут обеспечить надежную аутентификацию. Исходя из оценки риска, важно определить требуемой уровень защиты для выбора соответствующего метода аутентификации.

Средство автоматического подсоединения к удаленному компьютеру может предоставить способ получения неавторизованного доступа к бизнес-приложению. Следовательно, подключения к удаленным компьютерным системам необходимо аутентифицировать, что особенно важно, если подключение производится к сети, которая находится вне сферы контроля управления безопасностью организации.

11.4.3 Идентификация оборудования в сетях

Контроль

Автоматическая идентификация оборудования должна рассматриваться как средство аутентификации соединений, осуществляемых с определенных мест и с определенным оборудованием.

Руководство по внедрению

Идентификация оборудования в сетях – метод, который должен использоваться для того, чтобы сеанс мог быть инициирован только с определенного места или оборудования.

Встроенный или подсоединенный к терминалу идентификатор может использоваться для определения, разрешено ли этому конкретному терминалу инициировать или получать определенные сообщения.

Может быть необходимым применение физической защиты оборудования для обеспечения безопасности его идентификатора.

Прочая информация

Этот контроль может быть дополнен другими методами для проверки подлинности оборудования (11.4.2). Оборудование для идентификации может применяться в дополнение к аутентификации пользователей.

11.4.4 Защита диагностических и конфигурационных портов при удаленном доступе

Контроль

Физический и логической доступ к портам конфигурации и диагностики должен быть контролируемым.

Руководство по внедрению

Потенциальный контроль для обеспечения доступа к диагностическим и конфигурационным портам конфигурации включают в себя использование ключа и поддержку процедур для контроля физического доступа к порту. Примером такой поддержки процедур является обеспечение диагностики и конфигурации портов доступные только на основании договоренности между руководителем, отвечающим за

обеспечение компьютерных сервисов, и персоналом по поддержке аппаратных/программных средств обеспечения требующего доступа.

Порты, услуги и аналогичные средства, установленные на компьютере или в сети, которые не требуются для функционирования бизнеса, должны быть отключены или удалены.

Прочая информация

Многие компьютерные сети и системы связи имеют набор средств удаленной диагностики для использования инженерами по техобслуживанию. Будучи незащищенными, эти диагностические порты являются источником риска неавторизованного доступа.

11.4.5 Принцип разделения в сетях

Контроль

В сетях должны быть применены принципы разделения групп информационных услуг, пользователей и информационных систем.

Руководство по внедрению

Одно из таких мероприятий состоит в том, чтобы разделить их на отдельные логические сетевые домены, например, внутренний сетевой домен организации и внешние сетевые домены, каждый из которых защищен определенным периметром безопасности. Градуированная группа элементов управления может применяться в отдельных логических доменах сети для дальнейшего разделения сетевой безопасности, например, сети со свободным доступом, внутренних сетей, а также критически важных активов. Домены должны быть определены на основе оценки рисков и различных требований к безопасности в каждой из областей.

Такой периметр может быть реализован посредством внедрения шлюза безопасности между двумя связанными сетями для контроля доступа и информационного потока между ними. Этот шлюз следует конфигурировать для фильтрации трафика между доменами (11.4.6 и 11.4.7) и для блокировки неавторизованного доступа в соответствии с политикой контроля доступа организации (11.1). Примером такого шлюза является межсетевой экран. Другим способом изоляции отдельных логических доменов является ограничение доступа к сети с помощью виртуальных частных сетей групп пользователей внутри организации.

Сети могут также быть разделены с помощью функциональности сетевого устройства, например, IP коммутации. Отдельные домены могут быть реализованы путем управления сетью передачи данных потоков с использованием возможной маршрутизации/ коммутации, такие как списки контроля доступа.

Критерии для разделения сетей на домены следует формировать на основе анализа политики контроля доступа (10.1), а также учитывая влияние этого разделения на производительность в результате включения подходящей технологии маршрутизации сетей или шлюзов (11.4.6 и 11.4.7).

Кроме того, разделение сетей должны быть основаны на важности и классификации информации хранимой и обрабатываемой в сети с уровнем доверия или направлением бизнеса, с тем чтобы сократить последствия нарушения обслуживания.

Следует рассмотреть вопрос о разделении беспроводных сетей от внутренних и частных сетей. Так как периметры беспроводных сетей четко не определены, оценка рисков должна осуществляться для определения контроля (например, строгая аутентификация, криптографические методы и выбор частоты), чтобы поддерживать разделения в сетях.

Прочая информация

Компьютерные сети все более распространяются за пределы организации, поскольку создаются деловые партнерства, которые требуют общения между партнерами или

совместного использования сетевой инфраструктуры и средства обработки информации. Такие расширения увеличивают риск неавторизованного доступа к информационным системам сети, при чем в отношении некоторых из этих систем, вследствие их важности или критичности, может потребоваться защита от пользователей, получивших доступ к другим системам сети.

11.4.6 Контроль сетевых соединений

Контроль

Подключение пользователей к совместно используемым сетям, особенно к тем, которые выходят за территорию организации, необходимо ограничивать в соответствии с политикой контроля доступа и требованиями бизнес-приложений.

Руководство по внедрению

Права доступа к сети пользователей должны поддерживаться и обновляться в соответствии с политикой контроля доступа (11.1.1).

Возможность подключения пользователей могут быть ограничены через сеть шлюзов, которые фильтруют трафик с помощью определенных таблиц или правил. Примеры бизнес-приложений, к которым следует применять ограничения:

a) электронная почта;

b) передача файлов в одном направлении;

c) интерактивный доступ;

d) доступ к приложениям.

Соединение прав доступа к сети должны рассматриваться в определенное время суток.

Прочая информация

Требования политики контроля доступа для совместно используемых сетей, особенно тех, которые простираются за границы организации, могут потребовать внедрения дополнительных мероприятий по управлению информационной безопасностью, чтобы ограничивать возможности пользователей по подсоединению.

11.4.7 Управление маршрутизацией сети

Контроль

Маршрутизация средств управления должна быть осуществлена для обеспечения информационной безопасности, чтобы подсоединения компьютеров к информационным потокам не нарушали политику контроля доступа к бизнес-приложениям.

Руководство по внедрению

Обеспечение информационной безопасности при осуществлении маршрутизации основывается на надежном механизме контроля адресов источника и назначения сообщения.

Шлюзы безопасности могут быть использованы для проверки адреса источника и назначения на внутренние и внешние сети опорных точек, использующих прокси-сервер и/или сетевые технологии трансляции адресов. Необходимо, чтобы специалисты, занимающиеся внедрением, были осведомлены о характеристиках используемых механизмов. Требования по контролю за сетевой маршрутизацией должны основываться на политике контроля доступом (11.1).

Прочая информация

Сети совместного использования, особенно те, которые выходят за границы организации, могут требовать реализации мероприятий по обеспечению информационной безопасности при маршрутизации. Это является особенно важным для сетей совместно используемых с пользователями третьей стороны (не сотрудников организации).

11.5 Контроль доступа к операционной системе

Цель: Предотвратить несанкционированный доступ к операционным системам.

На уровне операционной системы следует использовать средства информационной безопасности для ограничения доступа к компьютерным ресурсам. Эти средства должны обеспечивать:

a) аутентификацию авторизованным пользователям, в соответствии с определенной политикой контроля доступа;

b) запись успешных и неудавшихся доступов в системе;

c) регистрацию использования специальных привилегий системы;

d) выдачу тревоги в случае нарушения политики безопасности системы;

e) обеспечение надлежащих средств для аутентификации;

f) ограничение времени подключения пользователей, в случае необходимости.

11.5.1 Безопасные процедуры регистрации с терминала

Контроль

Контроль доступа к операционным системам должен быть обеспечен безопасной процедурой регистрации.

Руководство по внедрению

Процедура регистрации в компьютерной системе следует проектировать так, чтобы свести к минимуму возможность неавторизованного доступа. Поэтому, процедура регистрации должна содержать минимум информации о системе, чтобы не оказывать помощи неавторизованному пользователю. Правильно спланированная процедура регистрации должна обладать следующими свойствами:

a) не отображать наименований системы или приложений, пока процесс регистрации не будет успешно завершен;

b) отображать общие уведомления, предупреждающее, что доступ к компьютеру могут получить только авторизированные пользователи;

c) не предоставлять сообщений-подсказок в течение процедуры регистрации, которые могли бы помочь неавторизованному пользователю;

d) подтверждать информацию регистрации только по завершении ввода всех входных данных. В случае ошибочного ввода система не показывает, какая часть данных является правильной или неправильной;

e) ограничивать число разрешенных неудачных попыток регистрации (рекомендуется три) и предусматривать:

1) запись неудачных и удачных попыток;

2) включение временной задержки прежде, чем будут разрешены дальнейшие попытки регистрации, или отклонение любых дальнейших попыток регистрации без специальной авторизации;

3) разъединение сеанса связи при передаче данных;

4) отправление тревожных сообщений на консоль (терминал), если достигнуто максимальное число попыток регистрации;

5) установление количества попыток паролей в сочетании с минимальной длины пароля и ценности защищаемой системы;

f) ограничивать максимальное и минимальное время, разрешённое для процедуры регистрации. Если оно превышено, система должна прекратить регистрацию;

g) фиксировать информацию в отношении успешной завершенной регистрации:

1) дату и время предыдущей успешной регистрации;

2) детали любых неудачных попыток регистрации, начиная с последней успешной регистрации;

h) не показывать введенный пароль или скрыть пароль символами;

i) не передавать пароли по сети открытым текстом.

Прочая информация

Если пароли передаются в открытом виде во время регистрации сеанса, то они могут быть перехвачены сетевой программой «Sniffer».

11.5.2 Идентификация и аутентификация пользователя

Контроль

Необходимо, чтобы все пользователи имели уникальный идентификатор (пользовательский ID) для их единоличного использования с тем, чтобы их действия могли быть проанализированы ответственным лицом.

Руководство по внедрению

Этот контроль должен применяться для всех типов пользователей (включая персонал технической поддержки, т.е. операторов, администраторов сети, системных программистов и администраторов баз данных).

Идентификаторы пользователей должны быть использованы для отслеживания деятельности ответственного лица. Мероприятия по обычному пользователю не следует проводить с привилегированными учетными записями.

В исключительных случаях могут быть использованы, где существует четкое преимущество ведения бизнеса, использование общих идентификаторов пользователя для групп пользователей или конкретного задания. В таких случаях, должны быть документированы утверждения руководства. Необходимы дополнительные элементы управления для поддержания подотчетности.

Общий идентификатор для использования отдельными лицами должны быть разрешены только там, где функции доступны и действия, совершаемые идентификатором не должны быть прослежены (например, доступ только для чтения), или, где есть и другие меры контроля на местах (например, пароль и регистрацию для общего ID выдается только на одного сотрудника один раз.

Там, где требуется высокий уровень аутентификации и проверки личности, должны быть использованы альтернативные методы аутентификации для паролей, таких как криптографические средства, смарт-карты, жетоны или биометрические средства.

Прочая информация

Пароли (11.3.1 и 11.5.3) – очень распространенный способ обеспечения идентификации и аутентификации, основанный на использовании пароля, который знает только пользователь. То же самое может быть достигнуто средствами криптографии и протоколами аутентификации. Прочность идентификации пользователя и проверка подлинности должны быть пригодны для конфиденциальности информации для получения доступа.

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

11.5.3 Система управления паролями

Контроль

Системы управления паролями должны интерактивными и обеспечивать высокое качество паролей.

Руководство по внедрению

Система управления паролями должна:

a) предписывать использование индивидуальных паролей для обеспечения установления ответственности;

b) позволять пользователям выбирать и изменять их собственные пароли, а также включать подтверждающую процедуру для учета ошибок ввода при необходимости;

c) предписывать выбор высококачественных паролей в соответствии с 11.3.1;

d) принуждать их к изменению паролей (11.3.1);

e) там, где пользователи выбирают пароли, обеспечивать изменение временных паролей при первой регистрации (11.2.3);

f) поддерживать хранение истории предыдущих пользовательских паролей (за предыдущий год) 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) форме.

Прочая информация

Пароли - одно из главных средств подтверждения полномочия пользователя, осуществляющего доступ к компьютерным сервисам. Для некоторых бизнес- приложений требуется назначение пользовательских паролей независимым должностным лицом; в таких случаях не применяются пункты b), d) и e) вышеизложенного руководства. В большинстве случаев пароли выбираются и поддерживаются пользователями. Руководство по использованию паролей в соответствии с 11.3.1.

11.5.4 Использование системных утилит

Контроль

Использование системных утилит, которые могут преодолеть средства контроля операционных систем и приложений, необходимо ограничивать и строго контролировать.

Руководство по внедрению

Необходимы следующие мероприятия для использования системных утилит:

a) использование процедур идентификации, аутентификации и авторизации системных утилит;

b) отделение системных утилит от прикладных программ;

c) ограничение использования системных утилит путем выбора минимального числа доверенных авторизованных пользователей (11.2.2);

d) авторизация эпизодического использования системных утилит;

e) ограничение доступности системных утилит, например, на время внесения авторизованных изменений;

f) регистрация использования всех системных утилит;

g) определение и документирование уровней авторизации в отношении системных утилит;

h) удаление или отключение всех ненужных утилит из системного программного обеспечения;

i) ограничение доступности использования системных утилит пользователями, имеющим доступ к прикладным системам, где требуется разделение режимов работы.

Прочая информация

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

11.5.5 Периоды бездействия в сеансах связи

Контроль

Необходимо обеспечить завершение сеансов связи после определенного периода бездействия.

Руководство по внедрению

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

обрабатываемой информации и используемых приложений, связанных с местом установки оборудования.

Некоторые персональные компьютеры обеспечивают ограниченную возможность блокировки оборудования по времени путем очистки экрана и предотвращения несанкционированного доступа, не осуществляя при этом закрытия сеанса приложений и сетевого сеанса.

Прочая информация

Оборудования, размещенные в местах повышенного риска, например в общедоступных местах или вне сферы контроля процесса управления безопасностью организации, обслуживающие системы высокого риска, должны отключаться после определенного времени их бездействия для предотвращения доступа неавторизованных лиц.

11.5.6 Ограничение времени соединения

Контроль

Ограничения подсоединения по времени должны обеспечивать дополнительную безопасность для приложений высокого риска.

Руководство по внедрению

Меру обеспечения информационной безопасности необходимо применять для наиболее важных компьютерных приложений, особенно тех, которые связаны с терминалами, установленными в местах повышенного риска, например, в общедоступных местах или вне сферы контроля управления безопасностью организации. Примеры таких ограничений:

a) использование заранее определенных отрезков времени, например, для пакетной передачи файлов или регулярных интерактивных сеансов небольшой продолжительности;

b) ограничение времени подключений часами работы организации, если нет необходимости сверхурочной или более продолжительной работы;

c) повторная аутентификация в равные промежутки времени.

Прочая информация

Ограничение периода времени, в течение которого разрешены подсоединения терминалов к компьютерным сервисам, уменьшает интервал времени, в течение которого возможен неавторизованный доступ. Ограничение продолжительности активных сеансов препятствует пользователей возможности держать работы сеансов открытыми, чтобы предотвратить повторную аутентификацию.

11.6 Контроль доступа к прикладным системам и информации

Цель: Предотвратить несанкционированный доступ к прикладным системам и информации.

Необходимо применять меры обеспечения информационной безопасности для ограничения доступа к прикладным системам и информации. Логический доступ к программному обеспечению информации должен быть ограничен только авторизованными пользователями.

Для этого необходимо обеспечивать:

a) контроль доступа пользователей к информации и функциям бизнес-приложений в соответствии с определенной бизнес политикой контроля доступа;

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

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

11.6.1 Ограничение доступа к информации

Контроль

Пользователям бизнес-приложений, включая персонал поддержки и эксплуатации, следует обеспечивать доступ к информации и функциям этих приложений в соответствии с определенной политикой контроля доступа.

Руководство по внедрению

Ограничения доступа должны быть основаны на требованиях к отдельным бизнес-приложениям (11.1).

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

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

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

c) контроль права доступа других приложений;

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

11.6.2 Изоляция систем, обрабатывающих важную информацию

Контроль

Системы, обрабатывающие важную информацию, должны быть обеспечены выделенной (изолированной) вычислительной средой.

Руководство по внедрению

Для изоляции систем необходимо учитывать следующее:

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

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

Прочая информация

Некоторые прикладные системы имеют очень большое значение с точки зрения безопасности данных и поэтому требуют специальных условий эксплуатации. Важность обрабатываемой информации может свидетельствовать о том, что применение системы должна:

a) требовать работы системы на выделенном компьютере; или

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

Изоляция систем может быть достигнута с помощью физических или логических методов (см. 11.4.5).

11.7 Работа с переносными устройствами и работа в дистанционном режиме

Цель: Обеспечить информационную безопасность при использовании переносных устройств и средств, необходимых для работы в дистанционном режиме.

Необходимо соизмерять требуемую защиту со специфичными рисками работы. При использовании переносных устройств следует учитывать риски, связанные с работой в незащищенной среде, и применять соответствующие меры защиты. В случаях работы в дистанционном режиме организация должна предусматривать защиту как места работы, так и соответствующие меры по обеспечению информационной безопасности.

11.7.1 Работа с переносными устройствами и средствами связи

Контроль

Необходимо иметь в наличии формализованную политику для защиты от рисков при использовании средств связи и переносных устройств.

Руководство по внедрению

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

Политика использования переносных устройств должна включать в себя требования по физической защите, контролю доступа, использованию средств и методов криптографии, резервированию и защите от вирусов. Эта политика также должна содержать правила и рекомендации по подсоединению мобильных средств к сетям, а также разработку руководства по использованию этих средств в общедоступных местах.

Следует проявлять осторожность при использовании мобильных средств вычислительной техники и других сервисных средств в общедоступных местах, переговорных комнатах и незащищенных помещениях вне организации. Чтобы исключить неавторизованный доступ или раскрытие информации, хранимой и обрабатываемой этими средствами, необходимо использование средств и методов криптографии (12.3).

При использовании мобильных средств в общедоступных местах важно проявлять осторожность, чтобы уменьшить риск «подсмотра» паролей доступа неавторизованными лицами. Необходимо внедрять и поддерживать в актуализированном состоянии средства и способы защиты от вредоносного программного обеспечения (см. 10.4).

Следует также обеспечивать доступность оборудования для быстрого и удобного резервирования информации. Необходимо также обеспечивать адекватную защиту резервных копий от кражи или потери информации.

Соответствующую защиту необходимо обеспечивать мобильным средствам, подсоединенным к общедоступным сетям. Удаленный доступ к служебной информации через общедоступную сеть с использованием мобильных средств вычислительной техники следует осуществлять только после успешной идентификации и аутентификации, а также при наличии соответствующих механизмов управления доступом (11.4).

Переносные устройства необходимо также физически защищать от краж, особенно когда их оставляют без присмотра, забывают в автомобилях или других видах транспорта, гостиничных номерах, конференц-залах и других местах встреч. Устанавливается определенная процедура на случай кражи или потери переносных устройств, учитывающая правовые требования, требования по страхованию и другие требования безопасности организации. Оборудование, на котором хранится важная и/или критическая коммерческая информация, не следует оставлять без присмотра и по возможности необходимо физически изолировать его в надежное место или использовать специальные защитные устройства на самом оборудовании, чтобы исключить его неавторизованное использование (9.2.5).

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

Прочая информация

Мобильная сеть беспроводного соединения схожи с другими типами сетей связи, но имеют особые различия, которые следует учитывать при определении мер контроля. Типичными различиями являются:

а) некоторые беспроводные протоколы безопасности являющиеся не сформированными и имеют известные недостатки;

б) информации, хранящиеся на мобильных компьютерах не могут быть резервной копией из-за ограниченной сети с пропускной способностью и/или потому что мобильное оборудование не может быть подключено во время резервных копий.

11.7.2 Работа в дистанционном режиме

Контроль

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

Руководство по внедрению

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

Следует обеспечивать защиту мест дистанционной работы как от краж оборудования и информации, так и от неавторизованного раскрытия информации, неавторизованного удаленного доступа к внутренним системам организации или неправильного использования оборудования. Важно, чтобы при работе в дистанционном режиме были выполнены требования как по авторизации, так и по контролю со стороны руководства, а также был обеспечен соответствующий уровень информационной безопасности этого способа работы.

Необходимо принимать во внимание:

а) существующую физическую безопасность места работы в дистанционном режиме, с точки зрения безопасности здания и окружающей среды;

b) предлагаемое оборудование мест дистанционной работы;

c) требования к безопасности коммуникаций, исходя из потребности в удаленном доступе к внутренним системам, организации, важности информации, к которой будет осуществляться доступ и которая будет передаваться по каналам связи, а также важность самих внутренних систем организации;

d) угрозу неавторизованного доступа к информации или ресурсам со стороны других лиц, имеющих доступ к месту дистанционной работы, например, членов семьи и друзей;

e) использование в домашних сетях требований или ограничений на конфигурацию беспроводных сетевых сервисов;

f) политику и процедуры для предотвращения споров о правах на интеллектуальную собственность разработанных на частное имущество;

g) доступ к частному оборудованию (для проверки безопасности компьютера или во время исследования), которые могут быть предотвращены законным путем;

h) лицензионные соглашения программного обеспечения, которые позволят организации стать ответственными за лицензирование программного обеспечения клиента на автоматизированных рабочих местах, принадлежавших конфиденциально сотрудникам, подрядчикам или пользователям сторонних организаций;

i) антивирусную защиту и систему сетевой защиты.

Мероприятия по обеспечению информационной безопасности в этих условиях должны включать:

а) обеспечение подходящим оборудованием и мебелью места дистанционной работы там, где использование оборудования, находящегося в частной собственности без контроля организации, не разрешается;

b) определение видов разрешенной работы, времени работы, классификацию, которая может храниться, а также определение внутренних систем и услуг, доступ к которым авторизован лицу, работающему в дистанционном режиме;

c) обеспечение подходящим телекоммуникационным оборудованием, в том числе средствами обеспечения безопасности удаленного доступа;

d) физическую безопасность;

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

f) обеспечение поддержки и обслуживания оборудования и программного обеспечения;

g) обеспечение страхования;

h) процедуры в отношении резервирования и непрерывности деятельности;

i) аудит и мониторинг безопасности;

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

Прочая информация

При работе используется технология связи, чтобы дать возможность персоналу работать в дистанционном режиме от установленного местоположения за пределами организации.

12 Разработка, внедрение и обслуживание информационных систем

12.1 Требования к безопасности информационных систем

Цель: Обеспечить уверенность в том, что безопасность является неотъемлемым свойством внедряемых информационных систем.

Эти требования касаются инфраструктуры, операционных систем, бизнес-приложений, а также приложений, разработанных пользователями. Процессы проектирования и внедрения бизнес-приложения или сервиса могут быть критичными с точки зрения безопасности. Требования к безопасности следует идентифицировать и согласовывать до разработки информационных систем. Все требования безопасности, включая необходимые мероприятия по переходу на аварийный режим, следует идентифицировать на стадии определения задач проекта, а также обосновывать, согласовывать и документировать в рамках общего проекта по внедрению информационной системы.

12.1.1 Анализ и детализация требований безопасности

Контроль

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

Руководство по внедрению

Следует учитывать возможности и необходимость применения организационных мероприятий по управлению информационной безопасностью или разработку специальных средств. Аналогично следует подходить к оценке пакетов прикладных программ, разработанных или приобретенных для служебного применения.

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

Планирование мероприятий по обеспечению информационной безопасности на стадии проектирования системы позволяет существенно снизить затраты на их внедрение и поддержку по сравнению с разработкой соответствующих мероприятий во время или после внедрения системы.

При приобретении программных продуктов необходимо осуществлять процесс официального тестирования и обслуживания. Контракты с поставщиком должны отвечать определенным требованиям безопасности. Когда функциональные возможности обеспечения безопасности предлагаемых продуктов не соответствуют указанным требованиям, то риски и связанные с ними введенные меры контроля, должны быть пересмотрены до приобретения продуктов. Если с программным продуктом поставляются дополнительные функциональные возможности и приводят к риску безопасности, то он должен быть заблокирован, или предлагаемая структура управления должна подлежать пересмотру для определения того, можно ли использовать улучшенные доступные функциональные возможности.

Прочая информация

Если считается целесообразным, например, по соображениям стоимости, руководство может использовать программные продукты, прошедшую независимую оценку и сертификацию. Дополнительная информация о критериях оценки для информационных технологий, приведена в СТ РК ИСО/МЭК 15408-1 или в других стандартах оценки и сертификации, по мере необходимости.

В СТ РК ИСО/МЭК ТО 13335-3 приведено руководство по использованию процессов управления рисками для идентификации требований по обеспечению информационной безопасности.

12.2 Правильная обработка данных в приложениях

Цель: Предотвратить ошибки, потерю, несанкционированную модификацию или неправильное использование информации в приложениях.

Соответствующие мероприятия по обеспечению информационной безопасности, включая функции аудита или протоколирование действий пользователя, необходимо предусматривать в прикладных системах, включая приложения, написанные самими пользователями. Эти меры должны включать в себя обеспечение функциональности подтверждения корректности ввода, обработки и вывода данных.

Дополнительные мероприятия по обеспечению информационной безопасности могут потребоваться для систем, которые обрабатывают или оказывают воздействие на важные, ценные или критические активы организации, и их необходимо определять на основе требований безопасности и оценки рисков.

12.2.1 Подтверждение корректности ввода данных

Контроль

Входные данные для приложений должны быть подвергнуты процедуре подтверждения с целью установления их достоверности.

Руководство по внедрению

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

a) проверки исключения двойного ввода или другие проверки ввода с целью обнаружения следующих ошибок:

1) значений, выходящих за допустимый диапазон;

2) недопустимых символов в полях данных;

3) отсутствующие или неполные данные;

4) превышение верхних и нижних пределов объема данных;

5) неавторизованные или противоречивые контрольные данные;

b) периодический анализ (просмотр) содержимого ключевых полей или файлов

данных для подтверждения их достоверности и целостности;

c) сверка твердых (печатных) копий вводимых документов с вводимыми данными на предмет выявления любых неавторизованных изменений этих данных (необходимо, чтобы все изменения во вводимых документах были авторизованы);

d) процедуры реагирования на ошибки, связанные с подтверждением данных;

e) процедуры проверки правдоподобия вводимых данных;

f) определение обязанностей всех сотрудников, вовлеченных в процесс ввода данных;

g) создание журнала для регистрации действий, вовлеченных в процесс ввода данных (10.10.1).

Прочая информация

Автоматическое испытание и проверка правильности входных данных можно рассматривать как уменьшение риска ошибок и предотвращение атак, включая стандартное переполнение буфера и введение кода.

12.2.2 Контроль обработки данных в системе

Контроль

Данные, которые были введены правильно, могут быть искажены вследствие ошибок обработки или преднамеренных действий. С целью обнаружения подобных искажений в функции систем следует включать требования, обеспечивающие выполнение контрольных проверок.

Руководство по внедрению

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

a) использование места в программах для функций добавления и удаления данных;

b) процедуры для предотвращения выполнения программ в неправильной последовательности или ее исполнения после сбоя на предыдущем этапе обработки данных (10.1.1);

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

d) защита против атак, используя переполнение буфера.

Должен быть подготовлен соответствующий список контрольных проверок, действия которых должны быть зарегистрированы и результаты сохранены:

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

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

1) средства контроля "от выполнения - к выполнению";

2) общие суммы измененных данных в файле;

3) средства контроля "от программы - к программе";

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

d) проверки целостности полученных или переданных данных (программного обеспечения) между центральным (главным) и удаленными компьютерами;

e) контрольные суммы записей и файлов;

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

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

h) создание журнала для регистрации действий, вовлеченных в процесс ввода данных (10.10.1).

Прочая информация

Данные, которые были введены правильно, могут быть искажены вследствие ошибок обработки и преднамеренных действий. Выбор необходимых средств контроля зависит от характера бизнес-приложения и последствий для бизнеса любого искажения данных.

12.2.3 Целостность сообщений

Контроль

Должны быть определены требования для обеспечения аутентичности и защиты целостности сообщений в приложениях, а также реализованы соответствующие средства контроля.

Руководство по внедрению

Оценка риска безопасности должна проводиться для определения целостности сообщений и подходящего способа реализации.

Прочая информация

При аутентификации сообщений могут использоваться криптографические методы защиты (12.3).

12.2.4 Подтверждение достоверности выходных данных

Контроль

Данные, выводимые из приложения, необходимо подвергать проверке на корректность, чтобы обеспечить уверенность в том, что обработка информации выполнена правильно.

Руководство по внедрению

Подтверждение корректности данных вывода может включать:

a) проверки на правдоподобие с целью определения, являются ли выходные данные приемлемыми;

b) проверки контрольных счетчиков на предмет удостоверения, что все данные были обработаны;

c) обеспечение достаточной информации для получателя результатов вывода или последующей системы обработки, чтобы определить корректность, законченность, точность и классификацию информации;

d) процедуры по выполнению тестов на подтверждение выводимых данных;

e) определение обязанностей всех сотрудников, вовлеченных в процесс вывода данных.

f) создание журнала регистрации действий в процессе подтверждения корректности вывода данных.

Прочая информация

Как правило, системы построены на предпосылке, что при наличии соответствующих подтверждений корректности, проверок и тестирования выводимые данные будут всегда правильны. Но это не всегда так, системы, которые прошли испытания могут выдавать неправильные данные при определенных обстоятельствах.

12.3 Криптографические средства защиты

Цель: Защитить конфиденциальность, аутентичность или целостность информации криптографическими средствами.

Необходимо разработать политику использования криптографических средств защиты информации. Управление ключами должно иметь место для поддержки использования криптографических методов.

12.3.1 Политика использования криптографических средств защиты

Контроль

Должны быть разработаны и внедрены правила использования криптографических средств защиты информации.

Руководство по внедрению

При разработке криптографической политики должно предусматриваться следующее:

a) подход руководства к использованию криптографических средств в организации, включая общие принципы, в соответствии с которыми следует защищать служебную информацию (5.1.1);

b) на основе оценки рисков необходимо определить требуемый уровень защиты, принимая во внимание тип и качество используемого алгоритма шифрования;

c) использование шифрования для защиты важной информации передаваемой на переносных или сменных носителях, устройствах или по линиям связи;

d) принципы управления ключами, включая методы работы с защитой криптографических ключей и восстановления зашифрованной информации в случае потери, компрометации или повреждения ключей;

e) функции и обязанности должностных лиц за:

1) реализацию политики;

2) управление ключами, включая генерацию ключей (12.3.2);

f) стандарты организации, которые будут приняты для эффективного осуществления в рамках всей организации (каждое решение используется для каждого бизнес-процесса);

g) последствия использования зашифрованной информации по элементам управления, которые полагаются на осмотр содержания (например, выявление вируса).

При разработке политики использования криптографических средств необходимо учитывать требования законодательства и ограничения, которые могут применяться в отношении использования криптографических методов в разных странах, а также вопросы, касающиеся объема потока зашифрованной информации, передаваемой через границы государств (15.1.6).

Криптографические средства защиты используются для целей безопасности, например:

a) конфиденциальность: использование шифрования информации в целях защиты критичной или важной информации, либо хранения или передачи;

b) целостность/аутентичность: использование цифровых подписей или кодов аутентификации сообщений для защиты подлинности и целостности хранения или передачи важной или критичной информации;

c) неотказуемость: использование криптографических методов для получения доказательств возникновения или не возникновения событий или действий.

Прочая информация

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

Политика использования криптографических средств необходима, чтобы максимизировать преимущества и минимизировать риски, связанные с использованием криптографических средств, а также избежать неадекватного или неправильного их использования. При использовании цифровых подписей необходимо учитывать

требования всех действующих законодательств, определяющих условия, при которых цифровая подпись имеет юридическую силу (15.1).

Для определения необходимого уровня защиты информации, выбора подходящих средств и методов защиты, которые должны обеспечивать требуемый уровень защиты и реализации безопасных способов управления ключами, целесообразно консультироваться со специалистами (12.3.2).

12.3.2 Управление ключами

Контроль

Для реализации организацией криптографических методов защиты должна быть использована система управления ключами.

Руководство по внедрению

Ключи необходимо защищать от изменения и разрушения, а секретным и личным ключам необходима защита от неавторизованного раскрытия. Физическую защиту следует применять для защиты оборудования, используемого для изготовления, хранения и архивирования ключей.

Необходимо, чтобы система обеспечения безопасности использования ключей основывалась на согласовании способов, процедур и безопасных методов для:

a) генерации ключей при использовании различных криптографических систем и различных приложений;

b) генерации и получения сертификатов открытых ключей;

c) рассылки ключей предназначенным пользователям, включая инструкции по их активации при получении;

d) хранения ключей; при этом необходимо наличие инструкции авторизованным пользователям для получения доступа к ключам;

e) смены или обновления ключей, включая правила порядка и сроков смены ключей;

f) порядка действий в отношении скомпрометированных ключей;

g) аннулирования ключей, в том числе способы аннулирования или дезактивации ключей, если ключи были скомпрометированы или пользователь уволился из организации (в этом случае ключи необходимо архивировать);

h) восстановления ключей, которые были утеряны или испорчены, для рассекречивания зашифрованной информации;

i) архивирования ключей, например для архивированной или резервной информации;

j) разрушения ключей;

k) регистрации и аудита действий, связанных с управлением ключами.

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

В дополнение к вопросу безопасности управления секретными и личными ключами необходимо учитывать необходимость обеспечения защиты открытых ключей. Существует угроза подделывания цифровой подписи и замены открытого ключа пользователя своим. Эта проблема решается с помощью сертификата открытых ключей. Этот процесс обычно выполняется уполномоченным органом по сертификации, который должен быть признанной организацией, руководствующейся соответствующими правилами и процедурами информационной безопасности для обеспечения требуемой степени доверия к нему.

Необходимо, чтобы содержание соглашений с внешними поставщиками криптографических средств, например, с уполномоченным органом по сертификации,

включало требования по ответственности, надежности средств и времени реагирования на запросы по их предоставлению (6.2.3).

Прочая информация

Управление криптографическими ключами важно для эффективного использования криптографических средств. Дополнительная информация об управлении ключами приведена в СТ РК ИСО/МЭК 11770-1. Следует применять систему защиты для обеспечения использования организацией следующих криптографических методов:

a) методы в отношении секретных ключей, где две или более стороны совместно используют один и тот же ключ, и этот ключ применяется как для шифрования, так и дешифрования информации. Этот ключ должен храниться в секрете, так как любой, имеющий доступ к этому ключу, может дешифровать всю информацию, зашифрованную с помощью этого ключа, или ввести неавторизованную информацию;

b) методы в отношении открытых ключей, где каждый пользователь имеет пару ключей, открытый ключ (который может быть показан любому) и личный ключ (который должен храниться в секрете). Методы с открытыми ключами могут использоваться для шифрования и для генерации цифровых подписей (см. ИСО/МЭК 9796-2, ИСО/МЭК 9796-3 и ИСО/МЭК 14888-1).

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

12.4 Безопасность системных файлов

Цель: Обеспечить безопасность системных файлов.

Доступ к системным файлам и исходным кодам программ должны контролироваться, и мероприятия по поддержке проектов информационных технологий должны проводиться в безопасном режиме. А также необходимо проявлять осторожность, чтобы избежать воздействия важных данных в среде тестирования.

12.4.1 Контроль программного обеспечения, находящегося в промышленной эксплуатации

Контроль

Необходимо обеспечить контроль за процессом внедрения программного обеспечения в промышленную эксплуатацию.

Руководство по внедрению

Чтобы свести к минимуму риск повреждения систем, находящихся в промышленной эксплуатации, целесообразно использовать следующие мероприятия по обеспечению информационной безопасности:

a) обновление библиотек программ следует выполнять только назначенному специалисту - библиотекарю при соответствующей авторизации его обязанностей руководством (12.4.3);

b) по возможности, системы, находящиеся в промышленной эксплуатации, должны состоять только из исполнимых программных кодов;

c) приложения и программное обеспечение операционной системы должны осуществляться только после длительного и успешного тестирования. Тестирования должны включать испытания на удобство, безопасность, воздействие на другие системы и удобство для пользователей, а также должно осуществляться на отдельных системах (см. 10.1.4). Необходимо обеспечить обновление всей исходной библиотеки программ;

d) следует использовать систему управления конфигурацией для сохранения контроля всех осуществляемых программ так же как системной документацией;

e) до начала осуществления изменений необходима стратегия возврата;

f) необходимо, чтобы журнал аудита регистрировал все обновления библиотек программ, находящихся в промышленной эксплуатации;

g) предыдущие версии программного обеспечения следует сохранять для восстановления системы в случае непредвиденных обстоятельств;

h) старые версии программного обеспечения необходимо архивировать, вместе со всей необходимой информацией и параметрами, процедурами, сведениями о конфигурации и поддержки программного обеспечения до тех пор, пока данные хранятся в архиве.

Необходимо, чтобы программное обеспечение, используемое в промышленной эксплуатации, поддерживалось на уровне, заданном разработчиком. Со временем, производители программного обеспечения прекращают поддержку старых версий программного обеспечения. Организация должна учесть риски полагаясь на неподдерживаемые программы.

При любом решении провести обновление до уровня новой версии следует принимать во внимание безопасность данной версии: какие новые функциональные возможности обеспечения информационной безопасности она имеет или имеются ли серьезные проблемы обеспечения безопасности, связанные с этой версией. Целесообразно использовать программные модификации (патчи), если они могут закрыть или снизить угрозы безопасности. (см. 12.6.1).

Физический или логический доступ предоставляется поставщикам (разработчикам), по мере необходимости, только для поддержки программного обеспечения при наличии разрешения руководства. При этом действия поставщика (разработчика) должны контролироваться.

Программное обеспечение, приобретенное сторонними организациями, занимающиеся поставкой программных продуктов и модулей, должны прослеживаться и контролироваться, чтобы избежать несанкционированных изменений, которые могут привести к угрозам безопасности.

Прочая информация

Операционная система должна обновляться, когда возникает при этом необходимость, например, если текущая версия операционной системы больше не поддерживает требования бизнеса. Обновления не должны иметь место только потому, что новая версия операционной системы доступна. Новые версии операционных систем могут быть менее безопасными, стабильными и понятными, чем существующие системы.

12.4.2 Защита данных тестирования системы

Контроль

Данные тестирования следует тщательно отбирать, защищать и контролировать.

Руководство по внедрению

Следует избегать использования баз данных, находящихся в промышленной эксплуатации и содержащих личную информацию. Если такая информация требуется для тестирования, то перед использованием следует удалить личную информацию (деперсонифицировать ее). Для защиты операционных данных, когда они используются для целей тестирования, необходимо применять следующие мероприятия по обеспечению информационной безопасности:

a) процедуры контроля доступа, применяемые для прикладных систем, находящихся в промышленной эксплуатации, следует также применять и к прикладным системам в среде тестирования;

b) при каждом копировании операционной информации для прикладной системы тестирования необходимо предусматривать авторизацию этих действий;

c) после того, как тестирование завершено, операционную информацию следует немедленно удалить из прикладной системы среды тестирования;

d) копирование и использование операционной информации необходимо регистрировать в журнале аудита.

Прочая информация

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

12.4.3 Контроль доступа к исходным кодам

Контроль

Доступ к исходным кодам должен быть ограничен.

Руководство по внедрению

Доступ к исходным кодам программ и связанные с ними элементы (такие, как дизайн, спецификации, планы проверок и утверждения планов) должны строго контролироваться, в целях предотвращения введения несанкционированного функционирования и во избежание непреднамеренных изменений. Для исходных кодов программ, это может быть достигнуто путем контролируемого централизованного хранения такого кода, предпочтительно в исходных библиотеках программ.

Для снижения риска искажения компьютерных программ необходимо обеспечивать строгий контроль доступа к библиотекам исходных текстов программ (Раздел 11), для чего:

a) по возможности, исходные библиотеки программ следует хранить отдельно от бизнес-приложений в промышленной эксплуатации;

b) исходными кодами и исходными библиотеками программ необходимо управлять в соответствии с установленными требованиями;

c) персоналу поддержки информационных технологий не следует предоставлять неограниченный доступ к исходным библиотекам программ;

d) обновление библиотек и обеспечение программистов исходными текстами и исходными кодами программ следует осуществлять после авторизации;

e) листинги программ следует хранить в безопасном месте (см. 10.7.4);

g) поддержку и копирование исходных библиотек следует проводить под строгим контролем с целью предотвращения внесения неавторизованных изменений (12.5.1).

Прочая информация

Исходные коды программы являются кодом, написанные программистами, которые составляются (и компонуются) для создания выполняемых программ. Некоторые языки программирования формально не различают исходный код и исполняемые файлы, поскольку они созданы в момент активации.

Дополнительная информация по управлению конфигурацией и процессом жизненного цикла программного обеспечения, приведена в СТ РК ИСО 10007 и ИСО/МЭК 12207.

12.5 Безопасность в процессах разработки и поддержки

Цель: Поддерживать безопасность программного обеспечения прикладных систем и содержащейся в них информации.

Среда проектирования или поддержки должны быть под строгим контролем.

Менеджеры, ответственные за прикладные системы, должны быть ответственными за безопасность среды проектирования или поддержки. Они должны проводить анализ всех предложенных изменений системы и исключать возможность компрометации безопасности как системы, так и среды промышленной эксплуатации.

12.5.1 Процедуры контроля изменений

Контроль

Внесение изменений должно быть проверено с использованием официальных соответствующих формализованных процедур контроля изменений.

Руководство по внедрению

Официальные процедуры контроля за внесением изменений должны быть документированы и приведены в исполнение в целях сведения к минимуму повреждения информационных систем. Введение новых систем и серьезных изменений в существующую систему должны следовать формализованной процедуре документации, технической характеристике, тестированию, контролю качества, и управляемому процессу внедрения.

Чтобы свести к минимуму повреждения информационных систем, следует строго контролировать внедрение изменений – строго придерживаться формализованных процедур обеспечения информационной безопасности; осуществлять контроль за возможной компрометацией самих процедур; программистам, отвечающим за поддержку, предоставлять доступ только к тем частям системы, которые необходимы для их работы; обеспечивать формализацию и одобрение соответствующим руководством всех изменений.

По возможности, следует объединять меры по обеспечению информационной безопасности используемых бизнес-приложений и изменений в прикладных программах (10.1.2). Необходимо, чтобы этот процесс включал:

a) обеспечение протоколирования согласованных уровней авторизации;

b) обеспечение уверенности в том, что запросы на изменения исходят от авторизованных соответствующим образом пользователей;

c) анализ мер информационной безопасности и процедур, обеспечивающих целостность используемых систем;

d) идентификацию всего программного обеспечения, информации, объектов, баз данных и аппаратных средств, требующих изменений;

e) получение формализованного одобрения детальных запросов/предложений на изменения перед началом работы;

f) разрешение внесения изменений в прикладные программы авторизованным пользователем до их непосредственной реализации;

g) обеспечение обновления комплекта системной документации после завершения каждого изменения и архивирования или утилизации старой документации;

h) поддержку контроля версий для всех обновлений программного обеспечения;

i) регистрацию в журналах аудита всех запросов на изменение;

j) коррекцию эксплуатационной документации (10.1.1) и пользовательских процедур в соответствии с внесенными изменениями;

k) осуществление процесса внедрения изменений в согласованное время без нарушения затрагиваемых бизнес-процессов.

Прочая информация

Изменения программного обеспечения могут повлиять на операционную среду.

Во многих организациях используется среда в которой пользователи тестируют новое программное обеспечение и которая отделена от среды разработки и среды промышленной эксплуатации (10.1.4). При этом обеспечивается возможность контроля нового программного обеспечения и дополнительная защита операционной информации, используемой в процессе тестирования.

Это должно включать патчи, пакеты программ и другие обновления. Автоматические обновления не следует использовать в критических системах некоторых обновлений, это может привести к сбоям критически важных приложений (см.12.6).

12.5.2 Технический анализ прикладных систем после внесения изменений в операционные системы

Контроль

При внесении изменений в операционные системы необходимо провести анализ и тестирование критичных бизнес-приложений с целью удостовериться в отсутствии негативного влияния на работу и безопасность организации.

Руководство по внедрению

Необходимо чтобы этот процесс учитывал:

a) анализ средств контроля бизнес-приложений и процедур целостности, чтобы обеспечить уверенность в том, что они были скомпрометированы изменениями в операционной системе;

b) обеспечение уверенности в том, что ежегодный план поддержки и бюджет предусматривает анализ и тестирование систем, которые необходимо осуществлять при изменениях в операционной системе;

c) обеспечение своевременного поступления уведомлений об изменениях в операционной системе для возможности проведения соответствующего анализа их влияния на информационную безопасность перед установкой изменений в операционную систему;

d) контроль документирования соответствующих изменений в планах обеспечения непрерывности бизнеса (Раздел 14).

Определенной группе или отдельным лицам должна возлагаться ответственность по контролю за уязвимостями и поставщиками патчей и их неисправностями (см. 12.6).

12.5.3 Ограничения на внесение изменений в пакеты программ

Контроль

Необходимо избегать модификаций пакетов программ, а все требуемые изменения должны подлежать строгому контролю.

Руководство по внедрению

Насколько это возможно и допустимо, поставляемые поставщиком пакеты программ следует использовать без внесения изменений. Там, где все-таки необходимо вносить изменения в пакет программ, следует учитывать:

a) риск компрометации встроенных средств и процесса обеспечения целостности;

b) необходимость получения согласия поставщика;

c) возможность получения требуемых изменений от поставщиков в виде стандартного обновления программ;

d) необходимость разработки дополнительных мер поддержки программного обеспечения, если организация в результате внесенных изменений станет ответственной за будущее сопровождение программного обеспечения.

В случае существенных изменений оригинальное программное обеспечение следует сохранять, а изменения следует вносить в четко идентифицированную копию. Программное обеспечение для управления процессом обновления должен быть выполнен для обеспечения наиболее современных утвержденных модификаций (патчи) и обновления приложений, установленных для всего авторизованного программного обеспечения (см. 12.6).

Все изменения необходимо полностью тестировать и документировать таким образом, чтобы их можно было повторно использовать, при необходимости, для будущих обновлений программного обеспечения. При необходимости, изменения должны быть проверены и подтверждены независимым органом оценки.

12.5.4 Утечка информации

Контроль

Возможности для утечки информации должны быть предотвращены.

Руководство по внедрению

Необходимо учитывать следующие ограничения риска утечки информации, например, на основе использования и эксплуатации скрытых каналов:

a) сканирование исходящей информации и связи для скрытой информации;

b) маскирующие и модулирующие системы и поведения связи, должны уменьшить вероятность того, что сторонняя организация, в состоянии вывести информацию от такого поведения;

c) использования систем и программного обеспечения, которые имеют высокий уровень целостности, например, оценка использования продуктов (см. СТ РК ИСО/МЭК 15408-1);

d) регулярный контроль персонала и системой деятельности, где это разрешено в рамках существующего законодательства или регулирования;

e) мониторинг использования ресурсов в компьютерных системах.

Прочая информация

Скрытые каналы являются путями, которые не предназначены для проведения информационных потоков, но тем не менее могут существовать в системе или сети. Например, манипулирование битами в коммуникационный протокол могут быть использованы программные пакеты в качестве метода скрытой передачи сигналов. По своей сути, предотвратить существование всех возможных скрытых каналов будет трудно и невозможно. Тем не менее, использование таких каналов зачастую осуществляется вредоносными «троянскими» программами (см. 10.4.1). Принимая меры по защите от «троянской» программы таким образом, снижается риск эксплуатации скрытых каналов.

Предотвращение несанкционированного доступа в сеть (см. 11.4), а также политики и процедуры со злоупотреблениями в использовании информационных служб по персоналу (15.1.5), поможет защититься от скрытых каналов.

12.5.5 Разработка программного обеспечения с привлечением сторонних организаций

Контроль

Разработка программного обеспечения с привлечением сторонних организаций должна проводиться под контролем и при мониторинге организации.

Руководство по внедрению

В случаях, когда для разработки программного обеспечения привлекается сторонняя организация, необходимо применять следующие меры обеспечения информационной безопасности:

a) контроль наличия лицензионных соглашений и определенности в вопросах собственности на программы и соблюдении прав интеллектуальной собственности (15.1.2);

b) сертификацию качества и правильности выполненных работ;

c) заключения «escrow» соглашения, предусматривающих депонирование исходного текста на случай невозможности сторонней организации выполнять свои обязательства;

d) обеспечение прав доступа для аудита с целью проверки качества и точности выполненной работы;

e) документирование требований к качеству программ в договорной форме;

f) тестирование перед установкой на предмет обнаружения вредоносного кода и «троянского коня».

12.6 Управление техническими уязвимостями

Цель: Снизить риски, являющиеся результатом использования опубликованных технических уязвимостей.

Управление технической уязвимостью должно быть реализовано в эффективном,

систематическом и повторяемом режиме с результатом измерений, принятых для подтверждения ее эффективности. Эти вопросы должны включать операционные системы и любые другие приложения в использовании.

12.6.1 Контроль технической уязвимости

Контроль

Необходимо получать своевременную информацию о технических уязвимостях используемых информационных систем, оценивать опасность таких уязвимостей и принимать соответствующие меры по устранению связанного с ними рисков.

Руководство по внедрению

Текущей и полной инвентаризацией активов (см. 7.1) является необходимым условием эффективного управления технической уязвимостью. Конкретные сведения, необходимые для поддержки управления технической уязвимости включает в себя программное обеспечение производителя, номер версии, текущее состояние развертывания (например, какое программное обеспечение установлено и на какие системы), а также персоналу в организации, ответственного за программное обеспечение.

Соответствующие и своевременные действия должны быть приняты в ответ на выявление потенциальных технических уязвимостей. Следующие рекомендации должны следовать для установления эффективного управления процесса технической уязвимости:

a) организация должна определить и установить роли и обязанности, связанные с управлением технической уязвимостью, включая мониторинг и оценку рисков уязвимости, обработку ошибок, отслеживание активов и любые требуемые обязанности по координации;

б) информационные ресурсы, которые будут использоваться для выявления соответствующих технических уязвимостей и поддержания осведомленности о них, должны быть определены в программном обеспечении или других технологиях (по инвентаризации активов, см. 7.1.1); эти информационные ресурсы должны обновляться с учетом изменений в кадастре, или при обнаружении других новых или полезных ресурсов;

c) необходимо определить время реагирования на уведомления о потенциально соответствующих технических уязвимостей;

d) как только потенциальная техническая уязвимость будет определена, организация должна определить риски и предпринять меры; такие меры могут включить корректировку уязвимых систем и/или применить другие виды контроля;

e) в зависимости от срочной технической уязвимости необходимо решать, какие меры контроля должны осуществляться, связанные с процедурами контроля изменений (см. 12.5.1) или процедурами реагирования на инциденты информационной безопасности (см. 13.2);

f) если патчи доступны, то риски, связанные с их установкой должны оцениваться (риски, связанные с уязвимостью следует сопоставить с риском установки патчей);

g) патчи должны быть проверены и оценены, прежде чем они будут установлены для обеспечения их эффективности, а также не приведут к побочным эффектам, которые не могут быть допущены, а если патчи не доступны, то должны быть рассмотрены другие меры контроля, например:

1) прекращение услуги или возможности, связанные с уязвимостью;

2) изменение или добавление контроля доступа, например, в системах сетевой защиты, на границах сетей (см. 11.4.5);

3) усиление мониторинга для обнаружения или предотвращения фактических атак;

4) повышение уровня осведомленности об уязвимости;

h) журналы аудита должны храниться в течение всех принятых процедур;

i) процесс управления технической уязвимости должен регулярно контролироваться и оцениваться с целью обеспечения ее эффективности и результативности;

j) системы с высоким риском должны быть рассмотрены в первую очередь.

Прочая информация

Правильное функционирование технологического процесса уязвимости управления организацией имеет важное значение для многих организаций и поэтому должны регулярно контролироваться. Точный учет в кадастре имеет существенное значение для обеспечения выявления потенциально соответствующих технических уязвимостей.

Управление технической уязвимостью может рассматриваться как подфункция управления изменениями, и как таковые могут использоваться в своих интересах процессы управления изменениями и процедуры (10.1.2 и 12.5.1).

Поставщики часто находятся под существенным давлением, чтобы выпустить патчи как можно скорее. Поэтому, обновление не может решить проблему соответствующим образом и могут быть отрицательные побочные эффекты. Кроме того, в некоторых случаях, удаление однажды примененных патчей, не могут быть легко достигнуты.

Если надлежащее тестирование патчей не возможно, например, из-за расходов или нехватки ресурсов, то задержки в исправлении можно рассматривать как оценку связанных с этим рисков, основанные на опыте о котором сообщают другие пользователи.

13 Управление инцидентами информационной безопасности

13.1 Оповещения о нарушениях и недостатках информационной безопасности

Цель: Обеспечить оперативность оповещения о событиях информационной безопасности и нарушениях, связанных с информационными системами, а также своевременность корректирующих действий.

Формализованные процедуры информирования об инцидентах и процедурах реагирования на инциденты должны быть в установленном порядке. Все сотрудники, подрядчики и пользователи сторонних организаций должны быть осведомлены о процедурах информирования о различных типах инцидентов нарушения информационной безопасности (угроза, уязвимость системы или сбой), которые могли бы оказать негативное влияние на безопасность активов организации. Сотрудники и подрядчики должны немедленно сообщать о любых наблюдаемых или предполагаемых инцидентах определенному контактному лицу или администратору безопасности.

13.1.1 Оповещение о случаях нарушения информационной безопасности

Контроль

О случаях нарушения информационной безопасности следует сообщать по соответствующим каналам управления незамедлительно, насколько это возможно.

Руководство по внедрению

Необходимо внедрить формализованную процедуру информирования об инцидентах, а также процедуру реагирования на инциденты, устанавливающие действия, которые должны быть предприняты после получения сообщения об инциденте. Для информирования об инцидентах нарушения информационной безопасности необходимо выбрать контактное лицо или администратора безопасности. Контактное лицо должно быть известно всей организации, всегда доступно и в состоянии обеспечить своевременное адекватное реагирование.

Все сотрудники и подрядчики должны быть ознакомлены с процедурой информирования об инцидентах нарушения информационной безопасности, а также проинформированы о необходимости незамедлительного сообщения об инцидентах. Они также должны быть осведомлены о процедуре информирования об инцидентах нарушения

информационной безопасности, а также сообщать контактному лицу или администратору безопасности. Процедура информирования должна включать:

a) предусмотреть процедуры обратной связи по результатам реагирования на инциденты нарушения информационной безопасности. После чего, этот вопрос должен быть решен и закрыт;

b) формы информирования об инцидентах нарушения информационной безопасности для поддержки действий информирования, и помощи информирующему лицу, чтобы он запомнил все необходимые действия в случае инцидентов нарушения информационной безопасности;

c) правильное поведение в случае инцидентов нарушения информационной безопасности, т.е.:

1) незамедлительно принимать к сведению все важные детали (например, тип несоответствия или нарушения, возникшие при сбоях системы, сообщения на экране, странное поведение);

2) не предпринимать самостоятельных действий, а следует немедленно известить соответствующее контактное лицо или администратора безопасности;

d) установление мер дисциплинарной ответственности сотрудников, подрядчиков или пользователей сторонних организаций, нарушивших требования безопасности.

В условиях повышенного риска, может быть установлен сигнал тревоги[3)] посредством чего человек под принуждением может указать на такие проблемы. Процедуры реагирования на сигналы принуждения должны отражать высокий риск ситуации.

Прочая информация

Примерами о событиях и инцидентах нарушения информационной безопасности являются:

a) потеря сервиса, оборудования или средств;

b) системные сбои или перегрузки;

c) человеческие ошибки;

d) несоблюдения политики или рекомендаций;

e) нарушения физических мер безопасности;

f) безудержные системные изменения;

g) сбои программного обеспечения или аппаратных средств;

h) нарушения прав доступа.

При должном внимании на аспекты конфиденциальности, инциденты информационной безопасности могут быть использованы в подготовке пользователей к осведомленности (см. 8.2.2) например того, что могло бы произойти, как реагировать на такие инциденты, и как избежать их в будущем. Чтобы иметь возможность правильно сообщить о событияях и инцидентах информационной безопасности, необходимо собрать доказательство как можно быстрее после их возникновения (см. 13.2.3).

Неисправности или другие неправильные режимы системы могут стать индикатором атаки безопасности или фактическими нарушениями безопасности, и, следовательно, должны быть сразу уведомлены как инциденты информационной безопасности.

Более подробная информация о регистрации событий информационной безопасности и управлении инцидентами безопасности, приведена в ИСО/МЭК ТО 18044.

[3)] Сигнал тревоги (duress alarms) является признаком того, что действие происходит «под принуждением» (under duress).

13.1.2 Оповещение о недостатках безопасности

Контроль

Все сотрудники, подрядчики и пользователи сторонних организаций, пользующиеся информационными системами и услугами, должны незамедлительно сообщать о любых замеченных или предполагаемых нарушениях безопасности в системах или услугах.

Руководство по внедрению

Для предотвращения нарушений информационной безопасности, сотрудники, подрядчики и пользователи сторонних организаций, должны сообщать незамедлительно об этих причинах для принятия решений своему руководству или непосредственно поставщику услуг. Механизм оповещения должен быть легким и доступным, насколько это возможно. Необходимо информировать пользователей, что они не должны ни при каких обстоятельствах пытаться доказать о предполагаемых недостатках в системе.

Прочая информация

Сотрудникам, подрядчикам и пользователям сторонних организаций рекомендуется не пытаться доказать о предполагаемых недостатках в системе безопасности.

Тестирование недостатков могли бы быть истолкованы в качестве потенциального злоупотребления системой и может также привести к повреждению системы информации или услуг и привести к правовой ответственности за отдельные выполнения тестирования.

13.2 Управление инцидентами информационной безопасности и его усовершенствование

Цель: Обеспечить последовательный и эффективный подход к управлению инцидентами информационной безопасности.

Обязанности и процедуры по управлению в отношении инцидентов должны быть определены для обеспечения быстрой и организованной реакции на эти нарушения информационной безопасности. Процесс непрерывного усовершенствования должен применяться к мониторингу, оценке и общему управлению инцидентами информационной безопасности.

Для обеспечения соблюдения правовых требований необходим сбор доказательств.

13.2.1 Ответственность и процедуры

Контроль

Должна быть установлена ответственность руководства и процедуры, позволяющие обеспечить быстрое, эффективное и последовательное реагирование на инциденты информационной безопасности.

Руководство по внедрению

В дополнение к оповещению о событиях информационной безопасности и нарушениях (см. также 13.1), для обнаружения инцидентов информационной безопасности, необходим мониторинг использования систем, предупреждения и уязвимостей (10.10.2).

В отношении инцидентов нарушения информационной безопасности должны рассматриваться следующие мероприятия:

а) должны быть определены процедуры в отношении всех возможных типов инцидентов нарушения информационной безопасности, в том числе:

1) сбои информационных систем и утраты сервисов;
2) от вредоносного кода (10.4.1);
3) отказ в обслуживании;
4) ошибки в вследствие неполных или неточных данных;
5) нарушения конфиденциальности и целостности;
6) злоупотребления информационными системами;

b) в дополнение к обычным планам обеспечения непрерывности, на случай непредвиденных ситуаций, (14.1.3) должны существовать процедуры выполнения требований (13.2.2):

1) анализ и идентификация причины инцидента;

2) ограничение распространения;

3) планирование и внедрение средств, предотвращающих повторное проявление инцидентов, при необходимости;

4) взаимодействия с лицами, на которых инцидент оказал воздействие участвующих в устранении последствий инцидента;

5) информирования о действиях соответствующих должностных лиц;

c) журналы аудита и аналогичные свидетельства должны быть собраны (13.2.3) и защищены соответствующим образом с целью:

1) внутреннего анализа проблемы;

2) использования как доказательство в отношении возможного нарушения условий контракта, нарушения требований законодательства или, в случае гражданских или уголовных судебных разбирательств, касающихся, например, защиты персональных данных или неправомочного использования компьютеров;

3) ведения переговоров относительно компенсации ущерба с поставщиками программного обеспечения и услуг;

d) действия по устранению сбоев систем и ликвидации последствий инцидентов нарушения информационной безопасности должны быть под тщательным и формализованным контролем. Необходимо наличие процедур с целью обеспечения уверенности в том, что:

1) только полностью идентифицированному и авторизованному персоналу предоставлен доступ к системам и данным в среде промышленной эксплуатации (6.2 в отношении доступа третьей стороны);

2) все действия, предпринятые при чрезвычайных обстоятельствах, подробно документально оформлены;

3) о действиях, предпринятых при чрезвычайных обстоятельствах, сообщено руководству организации, и они должны быть проанализированы в установленном порядке;

4) целостность бизнес-систем и система контроля подтверждены в минимальные сроки.

Цели в области управления инцидентами информационной безопасности должны быть согласованы с руководством и лицами, ответственными за управление инцидентами информационной безопасности, учитывая приоритеты организации для обработки этих инцидентов.

Прочая информация

Инциденты нарушения информационной безопасности могут выходить за пределы организационных и национальных границ. Для реагирования на такие инциденты существует растущая потребность в координации действий и обмена информацией об этих инцидентах с внедрением в сторонние организации.

13.2.2 Извлечение уроков из инцидентов информационной безопасности

Контроль

Должны быть определены механизмы позволяющие вести мониторинг и регистрацию инцидентов информационной безопасности по типам, объемам и стоимостям.

Руководство по внедрению

Информацию, полученную из оценки инцидентов информационной безопасности, следует использовать для идентификации повторяющихся или значительных инцидентов.

Прочая информация

Оценка инцидентов информационной безопасности может указывать на необходимость в совершенствовании существующих или внедрении дополнительных мероприятий по управлению информационной безопасностью с целью снижения возможного ущерба и расходов в будущем, кроме того, данную информацию следует учитывать при пересмотре политики информационной безопасности (5.1.2).

13.2.3 Сбор доказательств

Контроль

На случай, если инцидент информационной безопасности может привести к судебному разбирательству (гражданскому или уголовному) против лица или организации, информация должна быть собрана, сохранена и представлена согласно правилам оформления доказательств, изложенным в соответствующих документах.

Руководство по внедрению

При представлении и сборе доказательств в целях дисциплинарных мер, внутри организации следует разрабатывать и выполнять внутренние процедуры.

В общем случае, эти правила предусматривают:

a) допустимость свидетельств: действительно ли свидетельства могут использоваться в суде или нет;

b) весомость свидетельств: качество и полнота свидетельств.

Чтобы достичь признания допустимости свидетельств, организациям необходимо обеспечить уверенность в том, что их информационные системы соответствуют всем юридическим требованиям и правилам в отношении допустимых свидетельств.

Весомость свидетельств должна соответствовать требованиям действующего законодательства. Чтобы достичь качества и полноты свидетельств, необходимо наличие убедительных подтверждений свидетельств, что эти меры контроля (процесс сбора свидетельств) осуществлялись корректно и последовательно в течение всего периода, когда установленное свидетельство инцидента нарушения информационной безопасности было сохранено и обработано системой. В общем случае, такие убедительные подтверждения могут быть достигнуты следующим образом:

a) для бумажных документов: оригинал хранится безопасным способом и фиксируется, кто нашел его, где он был найден, когда он был найден и кто засвидетельствовал обнаружение. Необходимо, чтобы любое исследование подтвердило, что оригиналы никто не пытался исказить;

b) для информации на компьютерных носителях: копии информации, для любых сменных носителей информации, для жестких или из основной памяти компьютера, следует выполнять таким образом, чтобы обеспечить их доступность. Журнал всех действий, выполненных в течение процесса копирования, необходимо сохранять, а сам процесс копирования необходимо документировать. Одну копию носителей информации и журнал следует хранить безопасным способом.

Любая работа, связанная с судебным разбирательством, должна осуществляться только на копиях доказательного материала. Целостность всего доказательного материала должна быть защищена. Копирование материала должно контролироваться надежным персоналом, а информация о том, где и когда был проведен процесс копирования, кто осуществлял, какие инструменты и программы были при этом использованы, должны регистрироваться.

Прочая информация

Когда инцидент обнаруживается впервые, не очевидно, что он может привести к возможным судебным разбирательствам. Поэтому, существует опасность, что необходимое показание будет случайно разрушено прежде, чем осознана серьезность инцидента. Целесообразно на самом раннем этапе привлекать юриста или

правоохранительные органы в любом случае предполагаемых судебных разбирательств и получать консультацию относительно требуемых свидетельств.

Доказательство может выходить за пределы организационных и/или юрисдикционных границ. В таких случаях, следует обеспечить организации иметь право на сбор необходимой информации в качестве доказательства. Следует учитывать требования различных юрисдикций, чтобы придать огромное значение на признание доказательств действительными в соответствии с юрисдикцией.

14 Управление непрерывностью бизнеса

14.1 Вопросы информационной безопасности управления непрерывностью бизнеса

Цель: Противодействие прерываниям бизнеса и защита критических бизнес-процессов от последствий при значительных сбоях или бедствиях, а также обеспечение своевременного восстановления.

Необходимо обеспечивать управление непрерывностью бизнеса с целью минимизации отрицательных последствий, вызванных бедствиями и нарушениями безопасности (которые могут быть результатом природных бедствий, несчастных случаев, отказов оборудования и преднамеренных действий) до приемлемого уровня с помощью комбинирования предупреждающих и восстановительных мероприятий по управлению информационной безопасностью. Этот процесс должен определить критические бизнес-процессы и интеграции управления информационной безопасностью требованиям непрерывности бизнеса с другими требованиями непрерывности, касающиеся таких аспектов как операции, штатного расписания, материалы, транспорт и объектов.

Необходимо, чтобы управление непрерывностью бизнеса включало мероприятия по управлению информационной безопасностью для идентификации и уменьшения рисков, ограничения последствий разрушительных инцидентов и обеспечения своевременного возобновления наиболее существенных бизнес-операций.

Последствия от бедствий, нарушений безопасности и отказов в обслуживании необходимо анализировать. Необходимо разрабатывать и внедрять планы обеспечения непрерывности бизнеса с целью восстановления бизнес-процессов в течение требуемого времени при их нарушении. Такие планы следует поддерживать и применять на практике, чтобы они стали составной частью всех процессов управления.

14.1.1 Включение информационной безопасности в процесс управления непрерывностью бизнеса

Контроль

Необходимо, чтобы существовал управляемый процесс развития и поддержания непрерывности бизнеса для всей организации. Этот процесс должен объединять ключевые элементы управления непрерывностью бизнеса.

Руководство по внедрению

Этот процесс должен объединять ключевые элементы управления непрерывностью бизнеса:

a) понимание рисков, с которыми сталкивается организация, с точки зрения вероятности возникновения и последствий, включая идентификацию и определение приоритетов критических бизнес-процессов (14.1.2);

b) идентификацию всех активов, вовлеченных в критические бизнес-процессы (7.1.1);

c) понимание возможных последствий нарушения бизнес-процессов в случае незначительных или существенных инцидентов, потенциально угрожающих

жизнедеятельности организации, а также выбора средства и способов обработки информации, которые соответствовали бы целям бизнеса;

d) рассмотрение приобретения подходящей страховки, которая может быть частью полного процесса непрерывности бизнеса, как и частью оперативного управления риском;

e) идентификация и рассмотрение реализации дополнительных профилактических и смягчающих систем контроля;

f) организацию оптимального страхования безопасности персонала и имущества организации, а также результатов обработки информации, которое должно быть частью процесса обеспечения непрерывности бизнеса;

h) формулирование и документирование планов обеспечения непрерывности бизнеса, в соответствии с согласованной стратегией непрерывности бизнеса (14.1.3);

i) регулярное тестирование и обновление планов развития информационных технологий и существующих процессов (14.1.5);

j) обеспечение органичного включения в процессы и структуру организации планов управления непрерывностью бизнеса. Ответственность за координацию процесса управления непрерывностью бизнеса следует возлагать на орган, обладающий соответствующими полномочиями в организации (6.1.1).

14.1.2 Непрерывность бизнеса и оценка риска

Контроль

События, которые могут стать причиной прерывания бизнес-процессов, должны быть связаны с оценками вероятности и степени воздействия таких прерываний, а также с их последствиями для информационной безопасности.

Руководство по внедрению

Необходимо, чтобы планирование непрерывности бизнеса начиналось с идентификации событий, которые могут быть причиной прерывания бизнес-процессов, например отказ оборудования, воровство, пожар, природные катаклизмы или терроризм. Планирование должно сопровождаться оценкой рисков с целью определения возможности и последствий этих прерываний (как с точки зрения масштаба повреждения, так и периода восстановления).

Оценку рисков необходимо осуществлять при непосредственном участии владельцев бизнес-ресурсов и процессов. Оценка риска должна распространяться на все бизнес-процессы и не ограничиваться только средствами обработки информации, но должна включать результаты, определенные для информационной безопасности. Важно соединить различные аспекты риска, получить законченное изображение требований непрерывности бизнеса организации. Оценка должна идентифицировать, определить количество, и расположить по приоритетам риски против критериев и целей, относящихся к организации, включая критические ресурсы, воздействия разрушений, допустимое время выхода из строя, и приоритеты восстановления.

В зависимости от результатов оценки рисков необходимо разработать стратегию для определения общего подхода к обеспечению непрерывности бизнеса. Разработанный план должен быть утвержден руководством организации по выполнению данной стратегии.

14.1.3 Разработка и внедрение планов непрерывности бизнеса, включающих в себя информационную безопасность

Контроль

Следует разрабатывать планы непрерывности бизнеса по поддержке или восстановлению бизнес-операций в требуемые периоды времени после прерывания или отказа критических бизнес-процессов.

Руководство по внедрению

Необходимо, чтобы план обеспечения непрерывности бизнеса предусматривал следующие мероприятия по обеспечению безопасности:

a) определение и согласование всех обязанностей и процедур непрерывности бизнеса;

b) идентификацию приемлемых потерь информации и услуг;

c) внедрение процедур, обеспечивающих возможность восстановления бизнес-процессов и доступность информации в требуемое время. Особое внимание следует уделять оценке зависимости бизнеса от внешних факторов и существующих контрактов;

d) операционные процедуры, предназначенные для завершения процесса полного восстановления и восстановления потерянных данных;

e) документирование согласованных процедур и процессов;

f) соответствующее обучение сотрудников действиям при возникновении чрезвычайных ситуаций, включая кризисное управление;

g) тестирование и обновление планов обеспечения непрерывности бизнеса.

Необходимо, чтобы план обеспечения непрерывности бизнеса соответствовал требуемым целям бизнеса, например восстановлению определенных сервисов для клиентов за приемлемый промежуток времени. Следует учитывать потребности в необходимых для этого сервиса ресурсов, включая укомплектованные персоналом, альтернативными ресурсами для средств обработки информации, а также меры по переходу на аварийный режим работы для этих средств. Такие размещения системы восстановления могут включать размещения с третьими лицами в форме взаимных соглашений или рекламу подписных услуг.

Планы непрерывности бизнеса следует рассматривать как организационные факторы уязвимости и, следовательно могут содержать конфиденциальную информацию, которая должна быть надлежащим образом защищена. Копии планов непрерывности бизнеса должны храниться в достаточно отдаленном месте, чтобы избежать любого повреждения в результате бедствия в основном здании. Руководство должно гарантировать, что копии планов непрерывности бизнеса надежно защищены с тем же самым уровнем безопасности как применено в основном здании. Другие материалы, необходимые для выполнения планов непрерывности бизнеса следует хранить в достаточно отдаленном месте.

Если используются альтернативные временные места размещения, то уровень осуществленных управлений безопасности в этих местах должен быть эквивалентным уровню в основном здании.

Прочая информация

Необходимо отметить, что планы кризисного управления и действия (см. 14.1.3 f), могут отличаться от управления непрерывностью бизнеса, то есть кризис может произойти, который может быть приспособлен нормальными процедурами управления.

14.1.4 Структура планов обеспечения непрерывности бизнеса

Контроль

Следует поддерживать единую структуру планов обеспечения непрерывности бизнеса в целях обеспечения непротиворечивости всех планов и определения приоритетов для тестирования и обслуживания средств и систем обработки информации.

Руководство по внедрению

Необходимо, чтобы каждый план обеспечения непрерывности бизнеса определял подход к непрерывности, например, подход к обеспечению информации или доступности информационной системы и безопасности. Каждый план обеспечения непрерывности бизнеса должен четко определять условия его реализации, а также должностных лиц, ответственных за выполнение каждого его пункта. При выявлении новых требований необходимо вносить соответствующие корректировки в процедуры на случай чрезвычайных ситуаций, например в планы эвакуации или в любые существующие планы по переходу на аварийный режим работы. Процедуры должны быть включены в пределах

программы управления изменениями организации, чтобы гарантировать соответствующее направление для решения вопросов непрерывности бизнеса.

Необходимо, чтобы за каждый план отвечал конкретный руководитель (сотрудник). Чрезвычайные меры, планы по переходу на аварийный режим ручной обработки, планы по возобновлению работы следует включать в сферу ответственности владельцев соответствующих бизнес-ресурсов или участников затрагиваемых процессов. За меры по переходу на аварийный режим работы с использованием альтернативных технических средств, таких как средства обработки информации и связи, ответственность несут поставщики услуг.

Необходимо, чтобы структура планов обеспечения непрерывности бизнеса отвечала требованиям информационной безопасности и содержала следующее:

a) условия реализации планов, которые определяют порядок действий должностных лиц, которому необходимо следовать (как оценивать ситуацию, кто должен принимать участие, и т.д.) перед введением в действие каждого пункта плана;

b) процедуры на случай чрезвычайных ситуаций, которые должны быть предприняты после инцидента, подвергающего опасности бизнес-операции и/или человеческую жизнь;

c) процедуры перехода на аварийный режим работы, которые описывают необходимые действия по переносу важных бизнес-операций или сервисов-поддержки в альтернативное временное место размещения и по восстановлению бизнес-процессов в требуемые периоды времени;

d) временные операционные процедуры, обеспечивающие завершение полного восстановлении и восстановлении потерянных данных;

e) процедуры возобновления работы, которые описывают необходимые действия для возвращения к нормальному режиму ведения бизнеса;

f) график поддержки плана, который определяет сроки и методы тестирования, а также описание процесса поддержки плана;

g) мероприятия по обучению персонала, которые направлены на понимание процессов обеспечения непрерывности бизнеса сотрудниками, и поддержание постоянной эффективности этих процессов;

h) обязанности должностных лиц, ответственных за выполнение каждого пункта плана. При необходимости должны быть указаны альтернативные ответственные;

i) критические активы и ресурсы должны быть готовы к выполнению процедур, предусмотренных на случай чрезвычайной ситуации, систему восстановления и процедуры возобновления.

14.1.5 Тестирование, поддержка и пересмотр планов по обеспечению непрерывности бизнеса

Контроль

Планы по обеспечению непрерывности бизнеса необходимо регулярно тестировать и обновлять для обеспечения уверенности в их актуальности и эффективности.

Руководство по внедрению

Планы по обеспечению непрерывности бизнеса необходимо регулярно тестировать для обеспечения знания своих обязанностей всеми членами команды восстановления и другим персоналом, имеющим к этому отношение.

Необходимо, чтобы в графике тестирования плана по обеспечению непрерывности бизнеса указывалось, как и когда следует проверять каждый пункт плана. Необходимо обеспечить регулярное тестирование каждого пункта плана, при этом могут использоваться следующие методы:

a) тестирование ("имитация прогона") различных сценариев (обсуждение мер по восстановлению бизнеса на различных примерах прерываний);

b) моделирование (особенно для тренировки персонала по выполнению своих функций после инцидента и перехода к кризисному управлению);

c) тестирование технического восстановления (обеспечение уверенности в эффективном восстановлении информационных систем);

d) проверка восстановления в альтернативном месте (бизнес-процессы осуществляются параллельно с операциями по восстановлению в удаленном альтернативном месте);

e) тестирование средств и сервисов-поставщиков (обеспечение уверенности в том, что предоставленные сторонними организациями сервисы и программные продукты удовлетворяют контрактным обязательствам);

f) «генеральные репетиции» (тестирование того, что организация, персонал, оборудование, средства и процессы могут справляться с прерываниями).

Методы тестирования могут использоваться любой организацией и необходимо, чтобы они отражали специфику конкретного плана по восстановлению. Результаты тестирования должны записываться, и если это необходимо, следует принимать действия по усовершенствованию планов.

Необходимо назначать ответственных за проведение регулярных пересмотров плана по обеспечению непрерывности бизнеса. Идентифицированные изменения в бизнес-процессах, еще не отраженные в планах по обеспечению непрерывности бизнеса, должны быть учтены путем соответствующих обновлений планов. Формализованный процесс управления изменениями должен обеспечивать рассылку обновленных планов в рамках их регулярных пересмотров.

Примерами ситуаций, которые могли бы потребовать обновления планов, включают приобретение нового оборудования или обновление операционных систем, а также изменения связанные с:

a) персоналом;

b) адресами или номерами телефонов;

c) стратегией бизнеса;

d) местоположением, средствами и ресурсами;

e) законодательством;

f) подрядчиками, поставщиками и основными клиентами;

g) процессами (как новыми, так и изъятыми;

h) рисками (операционными и финансовыми).

15 Соответствие требованиям

15.1 Соответствие правовым требованиям

Цель: Предотвращение любых нарушений норм уголовного и гражданского права, обязательных предписаний и регулирующих требований или договорных обязательств, а также требований безопасности.

Проектирование и функционирование информационных систем, их использование и управление ими могут быть предметом обязательных предписаний, регулирующих требований, а также требований безопасности в договорных обязательствах.

Следует консультироваться с юристами организации или с практикующими юристами, имеющими соответствующую квалификацию, в отношении конкретных юридических вопросов. Следует иметь в виду, что законодательные требования в отношении информации, созданной в одной стране и переданной в другую страну (например, информационный поток, передаваемый за границу государства), различаются в разных странах.

15.1.1 Определение применимого законодательства

Контроль

Все применяемые нормы законодательства, обязательные предписания, регулирующие требования и договорные обязательства, следует четко определять и документировать для каждой информационной системы.

Руководство по внедрению

Конкретные мероприятия по обеспечению информационной безопасности и индивидуальные обязанности должностных лиц по выполнению этих требований необходимо соответствующим образом определять и документировать.

15.1.2 Права на интеллектуальную собственность (IPR)

Контроль

Должны быть внедрены соответствующие процедуры для применения законодательных, регулирующих и контрактных требований к используемым материалам с учетом прав на интеллектуальную собственность, а также прав на использование программных продуктов, являющихся предметом частной собственности.

Руководство по внедрению

Для защиты любых материалов являющихся интеллектуальной собственностью, необходимо предусматривать применение следующих мероприятий:

a) строгое следование требованиям авторского права на программное обеспечение, которое определяет законное использование программных и информационных продуктов;

b) определение порядка и правил приобретения программных продуктов;

c) обеспечение осведомленности сотрудников по вопросам авторского права на программное обеспечение принятых правил в отношении закупок, а также уведомление о применении дисциплинарных санкций к нарушителям;

d) ведение соответствующих регистров активов с требованиями защиты прав интеллектуальной собственности;

e) ведение подтверждений и доказательств собственности на лицензии, дистрибутивные диски, руководства и т.д.;

f) контроль за соблюдением ограничений максимального числа разрешенных пользователей программными продуктами;

g) регулярные проверки применения только авторизованного программного обеспечения и лицензированных продуктов;

h) реализация политики по обеспечению выполнения условий соответствующих лицензионных соглашений;

i) выполнение правил утилизации или передачи программного обеспечения в другие организации;

j) организация регулярного аудита;

k) соблюдение условий получения из общедоступных сетей программного обеспечения и информации;

l) не дублирование, преобразовывая в другой формат; извлечение из коммерческих записей (пленка, аудио), кроме определенного разрешения в соответствии с законом об авторском праве;

m) не копируя полностью или частично книги, статьи, отчеты или другие документы, кроме разрешенного в соответствии с законом об авторском праве;

Прочая информация

Права интеллектуальной собственности включают программное обеспечение или авторское право документа, права на проект, торговые марки, патенты, и лицензии исходного текста.

Программные продукты, являющиеся предметом собственности, обычно поставляются в рамках лицензионного соглашения, которое ограничивает использование

определенными компьютерами, а также могут ограничивать копирование их с целью создания резервных копий. Ситуация с правом на интеллектуальную собственность (IPR) программного обеспечения, разработанного организацией, требует разъяснения персоналу.

Законодательные, регулирующие и договорные требования могут вводить ограничения на копирование материалов, являющихся предметом собственности. В частности, эти ограничения могут содержать требования к использованию только тех материалов, которые или разработаны организацией, или лицензированы, или предоставляются разработчиком для организации.

15.1.3 Защита учетных записей организации

Контроль

Важные записи организации необходимо защищать от утраты, разрушения и фальсификации. В отношении некоторых данных может потребоваться обеспечение безопасности хранения с целью выполнения законодательных или регулирующих требований, а также поддержки бизнес-приложений.

Руководство по внедрению

Данные необходимо классифицировать по типам, например, бухгалтерские записи, записи баз данных, журналы транзакций, журналы аудитора и операционных процедур, каждый с указанием периодов хранения и типов носителей хранения данных (бумага, микрофильм, магнитные или оптические носители). Любые криптографические ключи, связанные с зашифрованными архивами или цифровыми подписями (12.3), следует хранить безопасным способом и предоставлять к ним, при необходимости, доступ только авторизованным лицам.

Следует учитывать возможность снижения качества носителя, используемых для хранения данных, осуществлять процедуры по хранению и уходу за носителями данных в соответствии с рекомендациями изготовителя. Для длительного хранения можно использовать бумагу и микрофиши.

При использовании электронных носителей данных следует применять процедуры проверки возможности доступа к данным (например, читаемость как самих носителей, так и формата данных) в течение всего периода их хранения с целью защиты от потери вследствие будущих изменений в информационных технологиях.

Системы хранения данных следует выбирать таким образом, чтобы требуемые данные могли быть извлечены способом с возможностью вывода всех необходимых записей в приемлемый период времени и в приемлемом формате, в зависимости от выполняемых требований.

Необходимо, чтобы система хранения обеспечила четкую идентификацию данных, а также период их хранения, установленных законом или регулирующими требованиями. Эта система должна представлять возможности по уничтожению данных после этого периода, когда у организации отпадет потребность в их хранении.

С целью выполнения данных обязательств организации следует:

a) разработать руководство в отношении сроков, порядка хранения и утилизации информации;

b) составить график хранения наиболее важных данных;

c) вести опись источников ключевой информации;

d) внедрить соответствующие меры для защиты важной информации от потери, разрушения и фальсификации.

Прочая информация

Для некоторых данных может потребоваться обеспечение безопасности хранения с целью выполнения законодательных или регулирующих требований, а также поддержки важных бизнес-приложений. В качестве примеров можно привести данные, которые могут

потребоваться как доказательства того, что организация работает в рамках установленных законом норм или регулирующих требований, или с целью адекватной защиты от гражданского или уголовного преследования, а также подтверждения финансового состояния организации для акционеров, партнеров и аудиторов. Период времени хранения и содержание данных могут быть установлены в соответствии с государственными законами или регулирующими требованиями. Дополнительная информация по управлению организационными данными приведена в СТ РК ИСО 15489-1.

15.1.4 Защита данных и конфиденциальность персональной информации

Контроль

Защита данных и конфиденциальность персональной информации должны быть обеспечены в соответствии с требованиями законов, нормативных актов и, где это применимо, в соответствии с положениями контрактов.

Руководство по внедрению

Защита данных организации и политики безопасности должны быть разработаны и внедрены. Эта политика должна быть доведена до всех заинтересованных лиц в обработке персональной информации.

Соответствие законодательству по защите данных требует соответствующей структуры управления информационной безопасностью. Лучше всего это достигается при назначении должностного лица, отвечающего за защиту данных путем соответствующего разъяснения менеджерам, пользователям и поставщикам услуг об их индивидуальной ответственности, а также обязательности выполнения соответствующих мероприятий по обеспечению информационной безопасности. Ответственность за обработку персональной информации и гарантировать понимание принципов защиты данных, а также знать применяемые нормы законодательства в отношении защиты личных данных. Должны быть осуществлены соответствующие технические и организационные меры для защиты персональной информации.

Прочая информация

В ряде стран введены нормы законодательства, в которых установлены ограничения в отношении обработки и передачи персональных данных (в основном, это касается информации о живущих людях, которые могут быть идентифицированы по этой информации). Такие ограничения могут налагать обязанности на тех, кто осуществляет сбор, обработку и распространение личной информации, а также могут ограничивать возможность передачи этих данных в другие страны.

15.1.5 Предотвращение нецелевого использования средств обработки информации

Контроль

Должны быть применены меры контроля для предотвращения нецелевого использования средств обработки информации.

Руководство по внедрению

Руководство должно определить уровни полномочий пользователей в отношении использования средств обработки информации. Любое использование этих средств для непроизводственных или неавторизованных целей, без одобрения руководства (6.1.4), следует расценивать как нецелевое. Если такая деятельность выявлена мониторингом или другими способами, то на это следует обратить внимание непосредственного руководителя сотрудника для принятия соответствующих мер дисциплинарного воздействия.

Перед осуществлением мониторинга необходимо получить консультацию юриста.

Все пользователи должны быть осведомлены о четких рамках разрешенного им доступа и мониторинга для обнаружения несанкционированного использования. Это может быть достигнуто, например, путем ознакомления пользователей с предоставленной

им авторизацией в письменной форме под роспись, в организации следует безопасным способом хранить копию этого документа. Сотрудники организации, подрядчики и пользователи сторонних организаций должны быть осведомлены о том, что во всех случаях они имеют право доступа только к тем данным, использование которых им разрешено.

Необходимо, чтобы при регистрации доступа к системе на экране компьютера было отражено предупреждающее сообщение, указывающее, что система, вход в которую пользователи пытаются осуществить, является системой с ограниченным доступом, и что неавторизованный доступ к ней запрещен. Пользователь должен подтвердить это прочтение и реагировать соответствующим образом на него, чтобы продолжить процесс регистрации (11.5.1).

Прочая информация

Средства обработки информации организации предназначены для обеспечения потребностей бизнеса.

Обнаружение вторжения, проверку информационного наполнения и другие инструменты мониторинга могут предотвратить и обнаружить неправильное употребление средств обработки информации.

Многие страны имеют или находятся в процессе введения законодательства по защите от неправильного использования компьютеров. Возможны случаи использования компьютера для неавторизованных целей с преступным умыслом.

Законность использования мониторинга зависит от действующего в стране законодательства и может потребоваться, чтобы сотрудники были осведомлены и дали документированное согласие на проведение мониторинга. Где используется вводимая система для открытого доступа (например, общественный Web-сайт) и подлежит мониторингу безопасности, и это сообщение должно быть отображено.

15.1.6 Регулирование использования средств криптографической защиты

Контроль

Мероприятия по обеспечению безопасности доступа к криптографическим средствам принимаются в соответствии с соглашениями, законами, регулирующими требованиями или другими инструментами.

Руководство по внедрению

В соответствии с соглашениями и законами по обеспечению безопасности доступа к криптографии принимаются следующие мероприятия:

a) ограничения импорта и/или экспорта аппаратных и программных средств для выполнения криптографических функций;

b) ограничения импорта и/или экспорта аппаратных и программных средств, которые разработаны таким образом, что имеют, как дополнение, криптографические функции;

c) ограничения на использование зашифровки;

d) обязательные или дискреционные методы доступа со стороны государства к информации, зашифрованной с помощью аппаратных и программных средств для обеспечения конфиденциальности ее содержания.

Для обеспечения уверенности в соответствии политики использования криптографических средств в организации национальному законодательству необходима консультация юриста. Прежде чем зашифрованная информация или криптографическое средство будут переданы в другую страну, необходимо также получить консультацию юриста.

15.2 Пересмотр политики безопасности и техническое соответствие требованиям безопасности

Цель: Обеспечить соответствие систем организационным политикам и стандартам безопасности.

Безопасность информационных систем необходимо регулярно анализировать и оценивать.

Такой анализ (пересмотр) необходимо осуществлять в отношении соответствующих политик безопасности, а программные средства и информационные системы должны подвергаться аудиту на предмет соответствия этим политикам.

15.2.1 Соответствие политикам и стандартам безопасности

Контроль

Руководители должны обеспечить, чтобы все процедуры безопасности в их сфере ответственности были выполнены правильно и соответствовали политикам и стандартам безопасности.

Руководство по внедрению

Руководители должны обеспечивать правильное выполнение всех процедур безопасности в пределах их зоны ответственности, на соответствие принятым политикам безопасности, стандартам безопасности и любым другим требованиям безопасности. Кроме того, все сферы деятельности организации необходимо подвергать регулярному пересмотру для обеспечения требований по обеспечению информационной безопасности.

Если какое-либо несоответствие найдено в результате пересмотра, то руководители должны:

a) определить причины этого несоответствия;

b) оценить потребность в действиях, для обеспечения того, чтобы несоответствие не повторилось;

c) определить и провести соответствующие корректирующие меры;

d) провести анализ предпринятых корректирующих действий.

Результаты пересмотра и корректирующих действий, выполненных руководителями, должны быть зарегистрированы и записаны. Менеджеры должны предоставлять отчет о результатах лицам, проводящим независимый аудит (6.1.8), если независимый аудит имеет место в области их ответственности.

Прочая информация

Вопросы мониторинга использования систем рассмотрены в Разделе 10.10.

15.2.2 Проверка технического соответствия требованиям безопасности

Контроль

Информационные системы следует регулярно проверять на соответствие требованиям стандартов безопасности.

Руководство по внедрению

Проверка технического соответствия должна осуществляться вручную (при помощи соответствующих инструментальных и программных средств, при необходимости) опытным системным инженером или с помощью автоматизированного пакета программ, который генерирует технический отчет для последующего анализа техническим специалистом.

Особую осторожность следует проявлять в случаях, когда тест на проникновение может привести к компрометации безопасности системы и непреднамеренному использованию других уязвимостей. Такие испытания должны быть запланированы, документированы и периодически повторяться.

Любая проверка технического соответствия должна выполняться только компетентными, авторизованными лицами под их наблюдением.

Прочая информация

Проверка технического соответствия включает испытания операционных систем для обеспечения уверенности в том, что мероприятия по обеспечению информационной безопасности функционирования аппаратных и программных средств были внедрены правильно. Этот тип проверки соответствия требует технической помощи специалиста.

Проверка соответствия также включает тестирование на наличие попыток несанкционированного доступа к системе (проникновение), которое может быть выполнено независимыми экспертами, специально приглашенными по контракту для этого. Данное тестирование может быть полезным для обнаружения уязвимостей в системе и для проверки эффективности мер безопасности при предотвращении неавторизованного доступа вследствие этих уязвимостей.

Тестирование на проникновение и оценка уязвимости позволяют создать снимок системы в определенном состоянии и в определенное время. Снимки ограничиваются теми частями системы, фактически проверенной по время попыток проникновения. Тестирование на проникновение и оценка уязвимости не являются заменой для оценки рисков.

15.3 Вопросы аудита информационных систем

Цель: Повышение эффективности процесса аудита информационных систем и снижение негативного влияния, связанного с данным процессом.

Необходимо предусмотреть мероприятия по обеспечению информационной безопасности операционной среды и инструментальных средств аудита в процессе проведения аудита систем.

Защита также требуется для поддержания целостности информационной системы и предотвращения неправильного использования инструментальных средств аудита.

15.3.1 Меры управления аудитом информационных систем

Контроль

Требования и процедуры аудита, включающие в себя проверки операционных систем, необходимо тщательно планировать и согласовывать, чтобы свести к минимуму риск прерывания бизнес-процессов.

Руководство по внедрению

Необходимо учитывать следующие мероприятия:

a) требования аудита необходимо согласовать с соответствующим руководством;

b) объем работ по проверкам следует согласовывать и контролировать;

c) при проведении проверок необходимо использовать доступ только для чтения к программному обеспечению и данным;

d) при проведении проверок необходимо использовать доступ только для чтения к программному обеспечению и данным. Другие виды доступа могут быть разрешены только в отношении изолированных копий файлов системы, которые необходимо удалять по завершению аудита;

e) необходимо четко идентифицировать и обеспечивать доступность необходимых ресурсов информационных систем для выполнения проверок;

f) требования в отношении специальной или дополнительной обработки данных следует идентифицировать и согласовывать;

g) весь доступ должен повергаться мониторингу и регистрироваться с целью обеспечения протоколирования для последующих ссылок;

h) все процедуры, требования и обязанности аудита следует документировать;

i) лицо(а), выполняющий аудит, должен быть независимым от проверяемой деятельности.

15.3.2 Защита инструментальных средств аудита информационных систем

Контроль

Доступ к инструментальным средствам аудита информационных систем необходимо защищать для предотвращения любой возможности их неправильного использования или компрометации.

Руководство по внедрению

Инструментальные средства необходимо отделять от систем разработки и систем операционной среды, а также не хранить эти средства в библиотеках магнитных лент или пользовательских областях, если не обеспечен соответствующий уровень дополнительной защиты.

Прочая информация

Если сторонняя организация привлечена к аудиту, то может возникнуть риск злоупотребления инструментами аудита и доступа к информации этой сторонней организацией. Меры контроля, такие как в 6.2.1 (оценка рисков) и 9.1.2 (ограничение физического доступа) могут рассматриваться для устранения рисков и должны предприниматься любые последовательные действия, такие как немедленное изменение пароля, раскрытого для аудиторов.

Указатель

К

П

Р

С

Т

У

Ф

Ц

Э

УДК 336.77:022:006.354 **МКС 35.040**

Ключевые слова: информационные технологии, информационная безопасность, риски, активы, охраняемая зона, контроль доступа, аудит, криптографические средства, управление ключами

Басуға _____ж. қол қойылды Пішімі 60х84 1/16
Қағазы офсеттік. Қаріп түрі «KZ Times New Roman»,
«Times New Roman»
Шартты баспа табағы 1,86. Таралымы ____ дана. Тапсырыс ____

«Қазақстан стандарттау және сертификаттау институты»
республикалық мемлекеттік кәсіпорны
010000, Астана қаласы Орынбор көшесі, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 240074