ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Информационная технология

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Практические правила управления информационной безопасностью

(ISO/IEC 27002:2013, MOD)

Издание официальное

Узбекское агентство стандартизации, метрологии и сертификации

Ташкент

Предисловие

1 РАЗРАБОТАН Государственным унитарным предприятием Центр научно-технических и маркетинговых исследований - «UNICON.UZ» (ГУП «UNICON.UZ»)

2 ВНЕСЕН Техническим комитетом по стандартизации в сфере информационных технологий и коммуникаций № 7

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») от 05.09.2016 № 05-784

4 Настоящий стандарт модифицирован по отношению к международному стандарту ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls (Информационные технологии. Методы обеспечения безопасности. Свод правил по управлению защитой информации).

Сведения о соответствии ссылочных международных стандартов государственным стандартам Республики Узбекистан приведены в дополнительном приложении А.

Полный перечень технических отклонений с объяснением причин их внесения приведен в дополнительном приложении В.

Перевод с английского языка (en).

Степень соответствия – модифицированная (MOD).

5 ВЗАМЕН O‘z DSt ISO/IEC 27002:2008

Содержание

Введение

1 Краткая информация и контекст

Настоящий стандарт, разработанный на основе O‘z DSt ISO/IEC 27001:201_, предназначен для использования в качестве рекомендаций по выбору организациями средств управления в процессе разработки и внедрения системы управления информационной безопасностью (СУИБ) или в качестве руководящего документа для организаций, внедряющих общепринятые средства управления информационной безопасностью. Настоящий стандарт также предназначен для использования при разработке рекомендаций по управлению информационной безопасностью для конкретных отраслей экономики и организаций с учетом их специфических потребностей и имеющихся рисков информационной безопасности.

Организации всех типов и размеров (в том числе государственные, частные, коммерческие и некоммерческие) собирают, обрабатывают, хранят информацию на электронных и физических носителях, а также передают и распространяют различную информацию, включая вербальную (например, на переговорах и презентациях).

Информация - это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления; например, знания, концепции, идеи и бренды относятся к нематериальным активам. Во взаимосвязанном мире информация и связанные с ней процессы обработки и защиты, системы, сети и персонал, обеспечивающий их функционирование, являются активами, которые, как и другие важные бизнес-активы организации, необходимо защищать от различных угроз.

Активы подвергаются как преднамеренным, так и случайным угрозам, а связанные с ними процессы, системы, сети и персонал имеют присущие им уязвимости. Изменения в бизнес-процессах и системах или другие внешние изменения (например, новые законодательные и нормативно-правовые акты) могут стать причиной возникновения новых рисков информационной безопасности. Следовательно, учитывая множество способов, с помощью которых угрозы могут быть реализованы посредством уязвимостей с целью нанести вред организации, риски нарушения информационной безопасности присутствуют всегда. Эффективное обеспечение информационной безопасности снижает эти риски, защищая организацию от угроз, а также уязвимостей, и уменьшая их воздействие на ее активы.

Информационная безопасность обеспечивается путем реализации соответствующего комплекса средств управления, которые могут быть представлены политиками, методами, процедурами, организационными структурами и функциями программного и аппаратного обеспечения. Для обеспечения необходимого уровня безопасности, соответствующего

бизнес-целям организации, указанные средства управления необходимо разрабатывать, внедрять, осуществлять их мониторинг, анализировать и совершенствовать.

В соответствии с требованиями O‘z DSt ISO/IEC 27001 организация должна внедрить систему управления информационной безопасностью (СУИБ), разработанную на основе всестороннего комплексного анализа рисков информационной безопасности организации, представляющую собой комплекс средств управления информационной безопасностью и являющуюся частью общей системы управления.

При проектировании многих информационных систем не были учтены требования O‘z DSt ISO/IEC 27001 и настоящего стандарта. Уровень безопасности, который может быть достигнут техническими средствами, имеет ряд ограничений и, следовательно, должен сопровождаться надлежащими средствами управления и процедурами. Выбор необходимых мероприятий по управлению информационной безопасностью требует тщательного планирования и детализации. Эффективная СУИБ нуждается в поддержке всего персонала организации. Кроме того, может потребоваться участие акционеров, поставщиков или других сторонних организаций. Кроме того, могут потребоваться консультации специалистов сторонних организаций.

Для того, чтобы активы организации были в достаточной мере безопасными и защищенными от ущерба, эффективную информационную безопасность, в более широком смысле, также обеспечивают руководство и другие заинтересованные стороны, которые тем самым выступают в качестве бизнес-партнеров.

2 Требования информационной безопасности

Организации важно определить свои требования информационной безопасности, учитывая при этом три важных фактора:

a) определение рисков организации, принимая во внимание глобальную стратегию бизнеса и цели организации. Посредством определения рисков происходит выявление угроз активам организации, оценка уязвимостей соответствующих активов и вероятности возникновения угроз, а также оценка возможных последствий;

b) требования законодательства, нормативно-правовых актов и договоров требования, которым должны удовлетворять организация, ее торговые партнеры, подрядчики и провайдеры услуг, а также социокультурная среда данных сторон;

c) набор принципов, целей и требований, разработанных организацией для поддержки своего функционирования.

Ресурсы, используемые при внедрении средств управления информационной безопасностью, должны быть пропорциональны размеру возможного ущерба, наносимого организации в результате нарушений

информационной безопасности при отсутствии этих средств управления. Результаты определения рисков помогут при определении конкретных мер и приоритетов в области управления рисками информационной безопасности, а также при внедрении средств управления, выбранных для минимизации этих рисков.

Рекомендации по управлению рисками информационной безопасности, в том числе рекомендации по определению, обработке, принятию, анализу рисков и по обмену информацией относительно рисков содержатся в O‘z DSt ISO/IEC 27005.

3 Выбор средств управления

Организации могут выбрать средства управления, представленные в настоящем стандарте или в других источниках, или для удовлетворения специфических потребностей, при необходимости, могут быть разработаны новые средства управления.

Выбор средств управления зависит от организационных решений, основанных на критериях приемлемости рисков, вариантах обработки рисков и общего подхода к управлению рисками, принятому в организации; при этом также необходимо учитывать требования соответствующих национальных и международных законодательных и нормативно-правовых актов. Выбор средств управления также зависит от способа их взаимодействия, чтобы обеспечить глубокую защиту.

Некоторые средства управления, приведенные в настоящем стандарте, могут рассматриваться как руководящие принципы для управления информационной безопасностью и применяться для большинства организаций. Подробная информация о выборе средств управления и различных вариантах обработки рисков приведена в O‘z DSt ISO/IEC 27005.

4 Разработка собственных руководств организации

Настоящий стандарт должен расцениваться как отправная точка для разработки рекомендаций под конкретные нужды организации. Не все средства управления и рекомендации, приведенные в настоящем стандарте, могут быть применимы.

Более того, могут потребоваться дополнительные средства управления и рекомендации, не включенные в настоящий стандарт. В документы, содержащие дополнительные рекомендации или средства управления, в соответствующих случаях полезно включать перекрестные ссылки на пункты настоящего стандарта, которые облегчат проверку соответствия, проводимую аудиторами и бизнес-партнерами.

5 Аспекты жизненного цикла

Информация имеет естественный жизненный цикл, начинающийся от ее создания и получения, далее включающий хранение, обработку, использование, передачу, и завершающийся ее уничтожением или порчей. Значение активов и риски для них могут варьироваться в течение их срока жизни (например, несанкционированное разглашение или кража финансовой отчетности компании станут гораздо меньше значимыми после их официального опубликования), но на всех этапах жизненного цикла активов остается важным обеспечение их информационной безопасности.

Жизненный цикл информационных систем представляет собой непрерывный процесс, включающий принятие решения об их создании, техническое задание, проектирование, разработка, тестирование, внедрение, использование, эксплуатация и заканчивающийся выводом из эксплуатации и утилизацией. Все этапы жизненного цикла должны выполняться с учетом требований информационной безопасности. Разработка новых и модернизация существующих систем предоставляют возможность организациям обновить и улучшить средства управления информационной безопасностью с учетом реальных инцидентов, а также существующих и прогнозируемых рисков информационной безопасности.

6 Взаимосвязанные стандарты

В то время как настоящий стандарт содержит рекомендации по целому комплексу средств управления информационной безопасностью, которые широко применяются во многих различных организациях, в остальных стандартах серии O‘z DSt ISO/IEC 27000 содержатся дополняющие друг друга рекомендации или требования к другим аспектам общего процесса управления информационной безопасностью.

Общее представление о СУИБ и стандартах этой серии можно получить из O‘z DSt ISO/IEC 27000, который кроме того содержит глоссарий терминов с соответствующими определениями, используемых в стандартах этой серии, а также описание областей применения и целей каждого ее стандарта.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Ахборот технологияси
ХАВФСИЗЛИКНИ ТАЪМИНЛАШ УСУЛЛАРИ
Ахборот хавфсизлигини бошқаришнинг амалий қоидалари

Информационная технология
МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
Практические правила управления информационной безопасностью

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

Дата введения 08.09.2016

1 Область применения

Настоящий стандарт содержит рекомендации, которые организации могут использовать при разработке своих стандартов информационной безопасности и правил управления информационной безопасностью, включая выбор, внедрение и управление средствами управления, с учетом имеющихся рисков информационной безопасности в среде организации.

Данный стандарт предназначен для использования организациями, которые намерены:

a) выбрать средства управления для эффективного функционирования СУИБ на основе требований O‘z DSt ISO/IEC 27001;

b) внедрить общепринятые средства управления информационной безопасностью;

c) разработать свои собственные рекомендации по управлению информационной безопасностью.

Издание официальное

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

O‘z DSt ISO/IEC 27000:2014 Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь

O‘z DSt ISO/IEC 27001:2016 Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования

O‘z DSt ISO/IEC 27005:2013 Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности

O‘z DSt ISO/IEC 27007:2015 Информационная технология. Методы обеспечения безопасности. Руководящие указания по аудиту систем управления информационной безопасностью

O‘z DSt ISO/IEC TR 27008:2015 Информационная технология. Методы обеспечения безопасности. Руководство для аудиторов по средствам управления, используемых в системах управления информационной безопасностью

O‘z DSt ISO/IEC 27031:2016 Информационная технология. Методы обеспечения безопасности. Руководящие указания по готовности информационно-коммуникационных технологий для ведения бизнеса

O‘z DSt ISO/IEC 27033-1:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 1. Обзор и концепции

O‘z DSt ISO/IEC 27033-2:2016 Информационная технология. Методы обеспечения безопасности. Защита сети. Часть 2. Руководящие указания по проектированию и внедрению защиты сети

O‘z DSt ISO/IEC 27033-3:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления

O‘z DSt ISO/IEC 27033-4:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 4. Коммуникации для обеспечения безопасности между сетями с применением шлюзов безопасности

O‘z DSt ISO/IEC 27033-5:2016 Информационная технология. Методы обеспечения безопасности. Безопасность информационной сети. Часть 5. Коммуникации для обеспечения безопасности между сетями с применением виртуальных частных сетей

O‘z DSt ISO/IEC 27035:2015 Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности

Примечание – При пользовании настоящим стандартом необходимо проверить действие ссылочных стандартов по указателю стандартов, составленному по состоянию на 1 января текущего года и по соответствующим информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по O‘z DSt ISO/IEC 27000.

4 Структура настоящего стандарта

Настоящий стандарт содержит 14 основных разделов с описанием средств управления информационной безопасностью, содержащих 35 главных категорий безопасности и 114 средств управления.

4.1 Разделы

Каждый раздел, определяющий средства управления информационной безопасностью, содержит одну или несколько главных категорий безопасности.

Порядок следования разделов настоящего стандарта не отражает их важности. В зависимости от обстоятельств, средства управления информационной безопасностью из некоторых или всех разделов могут быть важными, следовательно, каждой организации, применяющей настоящий стандарт, следует определить актуальные для нее разделы, их важность и применимость к отдельным бизнес-процессам. Кроме того, списки в настоящем стандарте не расположены в порядке приоритета.

4.2 Категории средств управления

Каждая главная категория средств управления информационной безопасностью содержит:

a) цель управления, формулирующую, что необходимо достичь;

b) одно или несколько средств управления, которые могут быть применены для достижения цели управления.

Описания средств управления представлены следующим образом.

Средство управления

Определяет конкретную формулировку средства управления для удовлетворения поставленных целей.

Руководство по внедрению

Предоставляет более подробную информацию по содействию внедрения средства управления и достижению поставленных целей. Руководство не может быть в полной и достаточной мере применено во всех ситуациях, а конкретные средства управления могут не удовлетворять требованиям организации.

Дополнительная информация

Приводится информация, которая возможно потребуется при рассмотрении, например, юридических вопросов и ссылок на другие стандарты. Если дополнительная информация не требуется, то эта часть исключается.

5 Политики информационной безопасности

5.1 Решение вопросов управления информационной безопасностью

Цель: Обеспечить решение вопросов управления и поддержки информационной безопасности в соответствии с требованиями бизнеса, законодательства и руководящих документов.

5.1.1 Политики информационной безопасности

Средство управления

Разработка, утверждение руководством, опубликование и доведение до сведения всего персонала организации и, при необходимости, сотрудников сторонних организаций политик информационной безопасности.

Руководство по внедрению

На самом верхнем уровне организация должна определить «политику информационной безопасности», которую утвердит ее руководство и в которой изложен подход организации к достижению целей в области информационной безопасности.

Политики информационной безопасности должны соответствовать требованиям, разработанным с учетом:

a) бизнес-стратегии;

b) законодательных, нормативно-правовых актов и договоров;

c) угроз информационной безопасности в существующей и проектируемой среде.

Политика информационной безопасности должна содержать положения, касающиеся:

a) определения информационной безопасности, целей и принципов руководства всеми видами деятельности, связанными с информационной безопасностью;

b) назначения общей и конкретной ответственности персонала при управлении информационной безопасностью для соответствующих ролей;

c) процессов обработки отклонений и исключений.

На более низком уровне политика информационной безопасности должна поддерживаться политиками по конкретным процедурам, связанным с обеспечением информационной безопасности; в этих политиках впоследствии будут предоставлены полномочия по внедрению средств управления информационной безопасностью, и они, как правило, будут структурированы с учетом удовлетворения потребностей определенных целевых групп внутри организации или выполнения конкретных процедур.

Примерами конкретных процедур, описываемых в отдельных политиках, являются:

a) управление доступом (раздел 9);

b) классификация (и обработка) информации (8.2);

c) физическая безопасность и безопасность окружающей среды (раздел 11);

d) процедуры, ориентированные на конечных пользователей, в том числе:

1) допустимое использование активов (8.1.3);

2) «чистый стол» и «чистый экран» (11.2.9);

3) передача информации (13.2.1);

4) мобильные устройства и дистанционная работа (6.2);

5) ограничения на установку и использование программного обеспечения (12.6.2);

e) резервное копирование (12.3);

f) передача информации (13.2);

g) антивирусная защита (12.2);

h) управление техническими уязвимостями (12.6.1);

i) криптографические средства защиты информации (раздел 10);

j) безопасность обмена информацией (раздел 13);

k) конфиденциальность и защита персональной информации (18.1.4);

l) отношения с поставщиками (раздел 15).

Эти политики должны быть доведены до сведения персонала организации и, при необходимости, сторонних организаций в доступной и понятной форме, например, в контексте «программы повышения осведомленности, обучения и тренингов в области информационной безопасности» (7.2.2).

Дополнительная информация

Необходимость во внутренних политиках информационной безопасности определяется самой организацией. Внутренние политики особенно важны для больших и более сложных организаций, в которых определение и утверждение предполагаемых уровней средств управления отделены от их внедрения, или в тех ситуациях, когда политика

распространяется на множество различных людей или функций организации. Политики информационной безопасности могут быть изданы в одном документе «Политика информационной безопасности», либо как комплект отдельных, но взаимосвязанных документов.

Если какая-либо из политик информационной безопасности распространяется за пределы организации, то следует соблюдать осторожность во избежание неразглашения конфиденциальной информации.

Некоторые организации используют другие названия для политик, например, «стандарты», «директивы» или «правила».

5.1.2 Пересмотр политик информационной безопасности

Средство управления

Пересмотр политик информационной безопасности через запланированные интервалы времени или при значительных изменениях для обеспечения их адекватности, достаточности и эффективности.

Руководство по внедрению

Необходимо, чтобы в организации были назначены ответственные должностные лица, которые должны отвечать за разработку, пересмотр и оценку политик информационной безопасности. В пересмотр следует включать определение возможностей улучшения политик информационной безопасности и подхода к управлению информационной безопасностью в зависимости от изменений организационной или технологической инфраструктуры, условий ведения бизнеса или требований законодательства.

При осуществлении пересмотра политик информационной безопасности следует принимать во внимание результаты анализа со стороны руководства.

Пересмотренные политики информационной безопасности должны быть утверждены руководством.

6 Организация обеспечения информационной безопасности

6.1 Внутренняя организация

Цель: Создать структуру управления, которая будет инициировать и управлять обеспечением информационной безопасности в организации.

6.1.1 Роли и ответственность в области информационной безопасности

Средство управления

Определение и распределение ответственности в области информационной безопасности.

Руководство по внедрению

Распределение ответственности в области информационной безопасности следует выполнять в соответствии с политиками информационной безопасности (5.1.1). Следует установить ответственность за защиту отдельных активов и выполнение конкретных процессов в области информационной безопасности. Следует установить ответственность за операции по управлению рисками информационной безопасности и, в том числе, за принятие остаточных рисков.

В случае необходимости ответственность следует дополнить более подробными рекомендациями для конкретных объектов и средств обработки информации. Следует определить локальную ответственность за защиту активов и выполнение конкретных процессов безопасности.

Должностные лица, ответственные за обеспечение информационной безопасности, могут делегировать выполнение задач в области информационной безопасности другим сотрудникам. Тем не менее, указанные должностные лица остаются ответственными и должны обеспечить правильное выполнение каждой делегированной задачи.

Следует определить области, за которые персонал несёт ответственность. В частности, следует выполнить следующие мероприятия:

a) установить и определить активы и процессы информационной безопасности;

b) назначить ответственного за каждый актив или процесс информационной безопасности, а также подробно задокументировать его ответственность (8.1.2);

c) определить и задокументировать уровни полномочий;

d) предоставить компетентным должностным лицам, назначенным ответственными в области информационной безопасности, возможность ознакамливаться с разработками;

e) установить и задокументировать действия по координации и контролю аспектов информационной безопасности при взаимоотношениях с поставщиками.

Дополнительная информация

Во многих организациях общая ответственность за разработку и внедрение системы обеспечения информационной безопасности, а также за оказание содействия в определении средств управления информационной безопасностью возлагается на администратора информационной безопасности.

Тем не менее, ответственность за определение подлежащих защите активов и внедрение средств управления часто несут руководители соответствующих подразделений. Распространенной практикой является назначение каждому активу владельца, который становится ответственным за его повседневную защиту.

6.1.2 Разграничение обязанностей

Средство управления

Разграничение взаимно противоположных обязанностей и областей ответственности для уменьшения возможности несанкционированной или непреднамеренной модификации или нецелевого использования активов организации.

Руководство по внедрению

Необходимо предпринимать меры предосторожности, чтобы ни один из сотрудников не мог иметь доступ к активам, модифицировать или использовать их без авторизации или обнаружения. Инициирование события должно быть отделено от его авторизации. При проектировании средств управления должна быть учтена возможность сговора.

Для небольших организаций разграничение обязанностей может оказаться труднодостижимым, однако данный принцип должен быть применен настолько, насколько это возможно и реально.

В тех случаях, когда разграничение обязанностей осуществить затруднительно, следует использовать другие средства управления, например, мониторинг деятельности, использование журналов аудита, а также мер административного контроля.

Дополнительная информация

Разграничение обязанностей является методом снижения случайного (непреднамеренного) риска или преднамеренно неправильного использования активов организации.

6.1.3 Связи с государственными органами

Средство управления

Поддержание надлежащих связей с соответствующими государственными органами власти и управления.

Руководство по внедрению

В организации должен быть установлен порядок, определяющий когда и кто должен связываться с государственными органами (например, органами внутренних дел, пожарной охраной, органами надзора), а также регламентирующий время сообщения об обнаруженных инцидентах информационной безопасности, если есть подозрения на нарушения законодательства.

Дополнительная информация

Для организаций, подвергающихся атаке через сеть Интернет, может потребоваться принятие мер против источника атаки со стороны государственных органов.

Поддержание связей с государственными органами должно осуществляться в соответствии с требованиями по управлению инцидентами информационной безопасности (раздел 16) и процессами обеспечения непрерывной работы и планирования чрезвычайных ситуаций (раздел 17). Связи с законодательными органами полезны для того, чтобы

принимать непосредственное участие в подготовке изменений в нормативно-правовые акты, которые должны соблюдаться организацией. К другим органам, с которыми необходимо поддерживать связи, можно отнести коммунальные службы, службы скорой помощи, управления пожарной охраны (относительно обеспечения непрерывности бизнеса), операторов телекоммуникаций (относительно маршрутизации и доступности соединительных линий), службы водоканала (относительно средств охлаждения для оборудования).

6.1.4 Связи со специальными группами по интересам

Средство управления

Поддержание надлежащих связей со специальными группами по интересам или профессиональными ассоциациями, участие в форумах специалистов по информационной безопасности.

Руководство по внедрению

Членство в специальных группах по интересам или форумах следует рассматривать как способ:

a) повышения осведомленности о передовых, современных практических решениях в области обеспечения информационной безопасности;

b) подтверждения того, что понимание среды информационной безопасности является современным и полным;

c) получения заблаговременных предупреждений об опасностях, рекомендаций и программных заплаток (патчей), относящихся к атакам и уязвимостям;

d) получения консультаций от специалистов по информационной безопасности;

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

f) налаживания контактов при возникновении инцидентов информационной безопасности (13.2.1).

Дополнительная информация

Для улучшения сотрудничества и координации вопросов по информационной безопасности могут быть заключены соглашения о совместном использовании информации. В данных соглашениях должны быть установлены требования по защите конфиденциальной информации.

6.1.5 Информационная безопасность при управлении проектами

Средство управления

Обеспечение информационной безопасности при управлении проектами независимо от типа проекта.

Руководство по внедрению

Информационная безопасность должна быть интегрирована в метод(ы) управления проектом организации, чтобы убедиться в том, что риски информационной безопасности были определены и отражены в

отдельном разделе проекта. Это требование обычно относится к любому проекту независимо от его типа, например, к проекту базового бизнес-процесса, информационной технологии (ИТ), управлению средствами и другими вспомогательными процессами. Используемые методы управления проектом должны требовать, чтобы:

a) цели информационной безопасности были включены в цели проекта;

b) определение рисков информационной безопасности было выполнено на раннем этапе проекта, чтобы идентифицировать необходимые средства управления;

c) информационная безопасность являлась частью всех фаз применяемой методологии проекта.

Во всех проектах должно быть учтено и периодически пересматриваться влияние информационной безопасности.

Ответственность за обеспечение информационной безопасности должна быть определена и распределена между конкретными ролями, определенными в методах управления проектом.

6.2 Мобильные устройства и дистанционная работа

Цель: Обеспечить безопасность дистанционной (удаленной) работы и использования мобильных устройств.

6.2.1 Политика использования мобильных устройств

Средство управления

Утверждение политики и принятие дополнительных мер безопасности для управления рисками, связанными с использованием мобильных устройств.

Руководство по внедрению

При использовании мобильных устройств следует соблюдать особую осторожность для предотвращения компрометации бизнес-информации. Политика использования мобильных устройств должна учитывать риски, связанные с работой с мобильными устройствами в незащищенных средах.

Политика использования мобильных устройств должна содержать:

a) регистрацию (серийные номера) мобильных устройств;

b) требования по физической защите;

c) ограничения по установке программного обеспечения;

d) требования к версиям программного обеспечения мобильного устройства и по применению программных заплаток;

e) ограничения на подключение к информационным сервисам;

f) средства управления доступом;

g) криптографические методы;

h) защиту от вредоносных программ;

i) дистанционное отключение, удаление информации или блокировку;

j) резервное копирование;

k) использование веб-сервисов и веб-приложений.

Следует соблюдать осторожность при использовании мобильных устройств в общественных местах, конференц-залах и других незащищенных помещениях вне организации. Следует внедрить защиту от несанкционированного доступа к мобильным устройствам или разглашения информации, хранимой и обрабатываемой этими устройствами, например, с помощью криптографических методов (раздел 10) и внедрения использования секретной информации аутентификации (9.2.4).

Мобильные устройства также необходимо физически защищать от краж, не рекомендуется оставлять их без присмотра, например, в автомобилях или других видах транспорта, гостиничных номерах, конференц-залах и местах проведения заседаний. На случаи кражи и потерь мобильных устройств следует утвердить определенный порядок с учетом требований законодательных актов, договоров страхования и других требований по безопасности организации. Мобильные устройства, содержащие конфиденциальную, закрытую и/или чувствительную бизнес-информацию, нельзя оставлять без присмотра и там, где это возможно, их следует прятать в сейф либо для безопасности устройства следует использовать специальную блокировку.

Для повышения осведомленности о дополнительных рисках, возникающих при дистанционной работе, и средствах управления, которые следует внедрять для персонала, пользующегося мобильными устройствами, следует устраивать тренинги.

В тех случаях, когда политика использования мобильных устройств разрешает использование персоналом принадлежащих ему мобильных устройств, в политике и соответствующих мерах безопасности также должно быть учтено следующее:

a) разграничение использования устройств в личных и бизнес-целях, в том числе использование программного обеспечения, поддерживающего такое разграничение и защиту бизнес-информации на устройстве, принадлежащем сотруднику;

b) обеспечение доступа пользователей к бизнес-информации только после подписания с ними так называемого «Соглашения с конечным пользователем», в котором пользователь подтверждает свои обязанности (физическая защита, обновление программного обеспечения и т. п.), отказывается от права собственности на бизнес-данные, разрешает дистанционно удалять данные организации в случае кражи или пропажи устройства или запрета на использование сервиса.

В политике использования мобильных устройств должны быть также учтены требования законодательства о персональных данных.

Дополнительная информация

Беспроводное подключение мобильного устройства подобно другим типам сетевого подключения, но имеет важные отличия, которые следует учитывать при выборе средств управления. К типичным отличиям относятся:

a) протоколы безопасности беспроводных сетей не надежны и имеют известные слабости;

b) информация, хранимая на мобильном устройстве, не может быть скопирована из-за ограниченной ширины полосы частот беспроводной сети или из-за того, что это устройство невозможно подключить в тот момент времени, на который запланировано резервное копирование.

Мобильные устройства обычно выполняют общие функции, например, работа в сети, доступ в сеть Интернет, электронная почта, обработка файлов, которые используются и в стационарных устройствах.

Для противодействия угрозам, возникающим при использовании мобильных устройств за пределами помещений организации, обычно используются те же средства управления информационной безопасностью, что и для стационарных устройств.

6.2.2 Дистанционная работа

Средство управления

Внедрение политики и принятие дополнительных мер безопасности для защиты получаемой, обрабатываемой и хранимой информации в местах дистанционной работы.

Руководство по внедрению

Если организация заключила с удаленным работником трудовой договор, то он должен быть ознакомлен с политикой, в которой определены условия и ограничения выполнения дистанционной работы. Если признана необходимость дистанционной работы, и она разрешена законодательством, следует учитывать следующие факторы:

a) существующая физическая безопасность места дистанционной работы с учетом физической безопасности здания и локальной среды;

b) предполагаемая физическая среда дистанционной работы;

c) требования к безопасности обмена информацией с учетом потребности в удаленном доступе ко внутренним системам организации, чувствительности доступной и передаваемой по каналам сетей телекоммуникаций общего пользования, в том числе сети Интернет, информации, а также чувствительности внутренней системы;

d) обеспечение виртуального доступа к рабочему столу, который предотвращает обработку и хранение информации о принадлежащем удаленному работнику оборудовании;

e) угроза несанкционированного доступа к информации или ресурсам других лиц, находящихся в этом же помещении, например, членов семьи и друзей;

f) использование домашних сетей, а также требования или ограничения к конфигурации сервисов беспроводных сетей;

g) политики и процедуры, предотвращающие возникновение разногласий относительно прав на интеллектуальную собственность разработки, выполненной на принадлежащем удаленному работнику оборудовании;

h) доступ к принадлежащему удаленному работнику оборудованию (для проверки безопасности машины или при проведении обследования) в нарушение действующего законодательства;

i) наличие лицензионных соглашений на использование программного обеспечения вследствие того, что организации могут стать ответственными за лицензирование программного обеспечения клиента на рабочих станциях, принадлежащих ее персоналу или пользователям сторонних организаций;

j) защита от вредоносных программ и требования к межсетевому экрану.

Кроме того, следует учитывать следующие рекомендации и организационные вопросы:

a) обеспечение необходимым для дистанционной работы оборудованием и сейфом, в тех случаях, когда не допускается использование не контролируемого организацией оборудования, принадлежащего удаленному работнику;

b) оформление разрешения на выполнение работ, режим работы, классификация информации, которую можно использовать, внутренние системы и сервисы, на доступ к которым удаленный работник будет иметь полномочия;

c) обеспечение необходимым оборудованием связи, в том числе методами безопасного удаленного доступа;

d) физическая безопасность;

e) правила и руководство по управлению доступом членов семьи и посетителя к оборудованию и информации;

f) обеспечение поддержки и эксплуатация программно-аппаратного обеспечения;

g) заключение договора страхования;

h) процедуры резервного копирования и обеспечения непрерывной работы;

i) аудит и мониторинг безопасности;

j) лишение удаленного работника полномочий и прав доступа, а также возврат оборудования при расторжении с ним трудового договора.

Дополнительная информация

Понятие «дистанционная работа» относится ко всем формам работы вне офиса, включая нетрадиционные рабочие среды, называемые, например, как «дистанционная передача данных», «гибкое рабочее место», «дистанционная работа» и «виртуальная работа».

7 Безопасность персонала

7.1 До трудоустройства

Цель: Обеспечить уверенность в том, что персонал и работающие по договору понимают свою ответственность и соответствуют тем должностям, на которые они рассматриваются.

7.1.1 Подбор персонала

Средство управления

Выполнение проверки достоверности биографий всех претендентов на трудоустройство, выполняемой в соответствии с законодательством, нормами, этикой и соразмерно требованиям бизнеса, классификации информации, подлежащей доступу, а также принимаемым рискам.

Руководство по внедрению

Проверку следует выполнять с учетом всех соответствующих мер по обеспечению конфиденциальности и защите персональных данных, требований законодательства о трудоустройстве, а также при наличии санкции. Следует проверять:

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

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

c) подтверждение заявляемого образования и профессиональной квалификации;

d) независимо - подлинность документов, удостоверяющих личность (паспорт или заменяющий его документ);

e) более тщательно - например, кредитную историю и наличие/отсутствие судимостей.

Когда претендент на трудоустройство претендует на конкретную роль в области информационной безопасности, организация должна убедиться в том, что:

a) этот претендент обладает необходимой компетентностью для выполнения этой роли;

b) этому претенденту можно доверить выполнение этой роли, особенно если эта роль является критической для организации.

В тех случаях, когда новому сотруднику непосредственно после приема на работу или в его процессе предстоит доступ к средствам обработки конфиденциальной информации, например, финансовой или совершенно секретной, следует выполнить специальную проверку.

В процедурах подбора следует определить критерии и ограничения на специальные проверки, например, кто имеет право выполнять подбор, а также как, когда и зачем выполняются специальные проверки.

Процесс подбора должен также выполняться и для работающих по договору. В этих случаях, в соглашении между организацией и работающим по договору должна быть определена ответственность за проведение подбора и процедуры уведомления, которые должны быть выполнены в том случае, если подбор не был завершен или если его результаты вызывают сомнения или беспокойство.

Информация по всем претендентам, рассматриваемым на замещение должностей внутри организации, должна собираться и обрабатываться в соответствии с действующим законодательством, которое существует в соответствующей юрисдикции. В зависимости от действующего законодательства, претенденты должны быть предварительно проинформированы о предпринимаемых действиях по проверке.

7.1.2 Условия трудового договора

Средство управления

Определение в трудовых договорах с персоналом и работающих по договору их ответственности и ответственности организации в области информационной безопасности.

Руководство по внедрению

В обязательствах из договоров для персонала и работающих по договору, кроме отражения политики информационной безопасности организации, следует осветить и сформулировать:

a) что всему персоналу и всем работающим по договору, которым предоставлен доступ к конфиденциальной информации, до предоставления доступа к средствам обработки информации следует подписать соглашение о конфиденциальности или неразглашении;

b) законные права и ответственность персонала, работающих по договору, например, относительно законодательства об авторских правах или о защите данных (18.1.2 и 18.1.4);

c) ответственность за классификацию информации и управление информацией организации, другими активами, связанными с информацией, средствами обработки информации и информационными сервисами, к которым обращаются персонал или работающие по договору (раздел 8);

d) ответственность персонала или работающих по договору за обращение с информацией, получаемой от других компаний или сторонних организаций;

e) меры, принимаемые в случае игнорирования требований по безопасности организации персоналом или работающими по договору (7.2.3).

Всех претендентов на трудоустройство предварительно следует ознакомить с ролями и ответственностью в области информационной безопасности.

Организации следует убедиться, что персонал и работающие по договору согласны с условиями относительно информационной безопасности в соответствии с видом и уровнем доступа, предоставляемого данным лицам к активам организации, связанными с информационными системами и сервисами.

При необходимости, ответственность должна сохраняться и в течение определенного срока после окончания трудовых отношений (7.3).

Дополнительная информация

Для описания ответственности персонала или работающих по договору относительно конфиденциальности, защиты данных, корпоративной этики, надлежащего использования оборудования и материально-технических средств организации может использоваться кодекс поведения, а также хорошо зарекомендовавшие себя практические правила, соблюдения которых требует организация.

Работающие по договору могут быть связаны с внешней организацией, от которой, в свою очередь, может потребоваться участие в договорных соглашениях от имени заключающего договор физического лица.

7.2 В период трудоустройства

Цель: Обеспечить уверенность в том, что персонал и работающие по договору осведомлены об их ответственности в области информационной безопасности и соблюдают политики информационной безопасности.

7.2.1 Ответственность руководства

Средство управления

Доведение до сведения персонала и работающих по договору требования руководства о необходимости относиться должным образом к безопасности в соответствии с утвержденными политиками и процедурами организации.

Руководство по внедрению

Область ответственности руководства должна включать требование по обеспечению того, чтобы персонал и работающие по договору:

a) были проинструктированы должным образом о своих ролях и ответственности в области информационной безопасности до предоставления им доступа к конфиденциальной информации или информационным системам;

b) получили рекомендации по безопасности, соответствующие их ролям в организации;

c) были мотивированы к выполнению политик информационной безопасности организации;

d) достигли уровня осведомленности, соответствующего их ролям и ответственности в организации (7.2.2);

e) соблюдали условия трудового договора, в том числе политику информационной безопасности организации, а также соответствующие методы работы;

f) продолжали приобретать соответствующие навыки и квалификацию, а также обучаться на регулярной основе;

g) имели возможность по анонимному телефону доверия сообщать о нарушениях политик или процедур информационной безопасности («информирование руководства о нарушениях»).

Дополнительная информация

Если персонал и работающие по договору не осведомлены о своей ответственности в области информационной безопасности, это может стать причиной значительного ущерба для организации. Мотивированный персонал, вероятно, будет более надежен, в результате чего количество инцидентов информационной безопасности, происходящих по вине персонала, значительно снижается.

Нетребовательность руководства может вызвать у персонала чувство недооцененности, отрицательно влияющее на информационную безопасность организации. Например, эта нетребовательность может привести к пренебрежению информационной безопасностью или потенциальному нецелевому использованию активов организации.

7.2.2 Осведомленность, обучение и тренинги в области информационной безопасности

Средство управления

Прохождение всего персонала организации, а там, где это необходимо, и работающих по договору, соответствующего обучения, а также регулярное получение ими обновленных вариантов политик и процедур информационной безопасности, принятых в организации и относящихся к их должностным обязанностям.

Руководство по внедрению

Программа повышения осведомленности в области информационной безопасности должна быть нацелена на повышение уровня знаний персонала организации, а при необходимости, и работающих по договору, об их ответственности в области информационной безопасности, а также на формирование необходимых навыков в этой области.

Программа повышения осведомленности в области информационной безопасности должна разрабатываться в соответствии с политиками информационной безопасности и соответствующими процедурами организации, а также с учетом необходимой защиты для информации организации и внедренных средств защиты информации. Программа повышения осведомленности должна включать различные мероприятия по повышению осведомленности, например, проведение тематических

мероприятий по наиболее актуальным вопросам информационной безопасности (таких как «день информационной безопасности»), выпуск буклетов или рассылка по электронной почте информационных писем.

Мероприятия программы повышения осведомленности должны планироваться с учетом различных ролей персонала организации и, при необходимости, предполагаемой осведомленности работающих по договору. Мероприятия программы повышения осведомленности должны планироваться на долгосрочную перспективу с определенной периодичностью, эти мероприятия при наличии возможности должны регулярно повторяться, чтобы обучить вновь принятых сотрудников и работающих по договору. При внесении изменений в политики и процедуры организации программа повышения осведомленности также должна оперативно корректироваться, она должна содержать обобщенный практический опыт, полученный при инцидентах информационной безопасности.

В соответствии с программой повышения осведомленности в области информационной безопасности следует проводить тренинги по повышению осведомленности. Формы проведения тренингов по повышению осведомленности могут быть различными: очное или дистанционное интерактивное обучение, вебинары, самостоятельное изучение учебных материалов и другие.

Во время обучения и тренингов в области информационной безопасности также должны рассматриваться общие вопросы информационной безопасности, например, такие:

a) заявление о приверженности руководства организации обеспечению информационной безопасности;

b) необходимость знать и выполнять применимые правила и должностные обязанности по информационной безопасности, определенные в политиках, стандартах, законодательных и нормативно-правовых актах, контрактах и соглашениях;

c) персональная подотчетность за собственные действия и бездействие, и общая ответственность за обеспечение безопасности или защиту информации, принадлежащей организации и сторонним организациям;

d) основные процедуры информационной безопасности (например, отчетность об инцидентах информационной безопасности) и основные средства управления (например, парольная защита, средства защиты от вредоносных программ и политика «чистого стола»);

e) материалы по информационной безопасности, содержащие контактную информацию, ресурсы для дополнительной информации и рекомендации, в том числе материалы по информационной безопасности для дальнейшего обучения и тренингов.

Обучение и тренинги в области информационной безопасности должны проводиться с определенной периодичностью. Сотрудники,

переведенные на другую должность или роль со значительно отличающимися требованиями информационной безопасности, наряду со стажерами, до вступления в новую должность должны пройти начальное обучение и тренинги.

Для эффективного обучения и тренингов организация должна разработать программу обучения и тренингов. Эта программа должна соответствовать политикам информационной безопасности и соответствующим процедурами организации, а также учитывать необходимость защиты информации организации и внедренные средства защиты информации. В программе должны быть предусмотрены различные формы обучения и тренингов, например, лекции или самообразование.

Дополнительная информация

При формировании программы повышения осведомленности важно сфокусироваться не только на «что» и «как», но и на «почему». Персонал должен четко понимать цель информационной безопасности и потенциальное влияние своего поведения, как положительное, так и отрицательное, на информационную безопасность организации.

Повышение осведомленности, обучение и тренинги в области информационной безопасности могут являться частью проводимого тренинга по совместной деятельности, например, общий тренинг по ИТ или по безопасности.

Осведомленность персонала, обучение и тренинги в области информационной безопасности должны быть приемлемыми и соответствовать его ролям, ответственности и навыкам.

По завершению курсов по повышению осведомленности, обучения и тренингов следует провести тестирование для оценки эффективности усвоения представленных материалов.

7.2.3 Меры дисциплинарного взыскания

Средство управления

Наличие официально оформленных мер дисциплинарного взыскания, которые заранее были доведены до сведения персонала, налагаемых на сотрудников, нарушивших политики и процедуры информационной безопасности, принятые в организации.

Руководство по внедрению

Не следует начинать дисциплинарную процедуру без предварительной проверки и твердой уверенности в том, что нарушение безопасности имело место (16.1.7).

Официальная дисциплинарная процедура должна обеспечивать объективное и справедливое отношение к персоналу, подозреваемому в совершении нарушения безопасности. Официальная дисциплинарная процедура должна предусматривать дифференцированные ответные меры, учитывающую такие факторы, как характер и серьезность нарушения и его

влияние на бизнес-деятельность, является ли данное нарушение первым или повторным, прошел ли нарушитель надлежащие тренинги, соответствующее законодательство, договоры в сфере бизнеса и, при необходимости, другие факторы.

Дисциплинарная процедура должна также использоваться как средство сдерживания, препятствующее нарушению политик и процедур информационной безопасности организации, а также любых других нарушений информационной безопасности. При преднамеренных нарушениях могут потребоваться безотлагательные действия.

Дополнительная информация

Дисциплинарная процедура также может стать дополнительной мотивацией или стимулом в том случае, когда предусмотрены меры поощрения за ответственное отношение к вопросам информационной безопасности.

7.3 Порядок прекращения трудового договора и перевода на другую работу

Цель: Защитить интересы организации при прекращении трудового договора или переводе на другую работу.

7.3.1 Ответственность при прекращении трудового договора или переводе на другую работу

Средство управления

Определение и доведение до сведения персонала или работающих по договору требования о том, что ответственность в области информационной безопасности и должностных обязанностей продолжает действовать и после прекращения трудового договора или перевода на другую работу.

Руководство по внедрению

Порядок прекращения трудового договора должен включать действующие требования информационной безопасности, юридическую обоснованность и ответственность, а при необходимости - ответственность, содержащуюся в соглашении о соблюдении конфиденциальности (13.2.4) и условиях трудового договора (7.1.2), распространяющиеся на определенный период после прекращения трудового договора с персоналом или работающими по договору.

Ответственность и должностные обязанности, остающиеся действительными после прекращения трудового договора, должны содержаться в условиях трудовых договоров персонала или работающих по договору.

Изменениями в ответственности или должности следует управлять также, как и завершением соответствующей ответственности или

должности, объединенным с инициацией новой ответственности или должности.

Дополнительная информация

Общую ответственность за процесс прекращения трудового договора в целом несет отдел кадров, действуя совместно с непосредственным руководителем увольняемого лица и предоставляя ему урегулирование связанных с информационной безопасностью аспектов соответствующих процедур. Процедура освобождения от обязанностей работающего по контракту может быть выполнена сторонней организацией в соответствии с договором между организацией и этой сторонней организацией.

При необходимости следует информировать персонал, заказчиков, работающих по договору об изменениях штатного расписания и выполняемой работы.

8 Управление активами

8.1 Ответственность за активы

Цель: Идентифицировать активы организации и определить соответствующую ответственность за их защиту.

8.1.1 Инвентаризация активов

Средство управления

Идентификация информации, других активов, связанных с информацией, и средств обработки информации, составление инвентаризационной описи этих активов и поддержание ее в актуальном состоянии.

Руководство по внедрению

Организация должна идентифицировать все активы с учетом жизненного цикла информации и документально зафиксировать важность этих активов. Жизненный цикл информации должен включать создание, обработку, хранение, передачу, удаление и уничтожение. Документация должна храниться должным образом в специальных или существующих архивах.

Инвентаризационная опись активов должна быть точной, актуальной, полной и составлена по установленной форме.

Для каждого идентифицированного актива должен быть назначен владелец (8.1.2), также каждый идентифицированный актив должен быть классифицирован (8.2).

Дополнительная информация

Инвентаризация активов помогает убедиться в том, что обеспечивается их эффективная защита, а также она может потребоваться

для других целей, например, для обеспечения безопасности труда, страхования или решения финансовых вопросов (управление активами).

При идентификации своих активов организация может воспользоваться примерами активов, приведенными в O‘z DSt ISO/IEC 27005. Процесс составления инвентаризационной описи активов является важным предварительным условием управления рисками (см. также O‘z DSt ISO/IEC 27000 и O‘z DSt ISO/IEC 27005).

8.1.2 Владение активами

Средство управления

Назначение владельцев активам, перечисленным в инвентаризационной описи.

Руководство по внедрению

Отдельные сотрудники, а также различные подразделения, назначенные руководством организации ответственными за жизненный цикл активов, обладают правами владельцев активов.

Процесс, обеспечивающий своевременное назначение владельцев активов, выполняется обычным порядком. Владельцы активов должны назначаться после создания или поступления активов в организацию. Владелец актива должен отвечать за соответствующее управление активом в течение всего его жизненного цикла.

Владелец активов должен:

a) обеспечить учет активов при инвентаризации;

b) обеспечить соответствующую классификацию и защиту активов;

c) определить и периодически просматривать ограничения на доступ и классификацию важных активов с учетом применяемых политик управления доступом;

d) обеспечить выполнение соответствующих операций при удалении или уничтожении активов.

Дополнительная информация

Владельцем активов может быть определен как отдельный сотрудник, так и подразделение, назначенные руководством организации ответственными за управление всем жизненным циклом активов. Назначенный владельцем активов необязательно обладает какими-либо правами собственности на эти активы.

Повседневные задачи могут быть делегированы, например, оператору, ежедневно следящему за активами, но ответственность остается за владельцем.

В сложных информационных системах, возможно, полезно будет определить группы совместно действующих активов, предоставляющих специфичные сервисы. В этом случае владелец сервиса является ответственным за предоставление этого сервиса, в том числе и за операции с предоставляющими его активами.

8.1.3 Допустимое использование активов

Средство управления

Четкое определение, документирование и внедрение правил допустимого использования информации и активов, связанных со средствами обработки информации.

Руководство по внедрению

Персонал и пользователи сторонней организации, пользующиеся активами организации или имеющие к ним доступ, должны быть осведомлены о требованиях по обеспечению информационной безопасности информации организации, других активов, связанных с информацией, средств обработки информации и ресурсов. Они также должны знать, что при обработке информации несут ответственность за любое использование ими любых ресурсов.

8.1.4 Возвращение активов

Средство управления

Обязательное возвращение всех активов организации, находящихся у персонала и пользователей сторонних организаций по окончании срока действия их трудового договора, контракта или соглашения.

Руководство по внедрению

Процесс прекращения трудового договора следует формализовать и обеспечить возврат всех выданных ранее материальных активов, в том числе электронных носителей, предоставленных организацией и принадлежащих ей.

В тех случаях, когда персонал или пользователи сторонней организации приобретают оборудование у организации или используют принадлежащее им оборудование, следует соблюдать процедуры, обеспечивающие передачу организации всей необходимой информации и ее надежное удаление из этого оборудования (11.2.7).

В тех случаях, когда персонал или пользователи сторонней организации обладают важными знаниями, необходимыми для выполнения текущей работы, эту информацию следует задокументировать и передать организации.

В период действия уведомления о прекращении трудового договора организация должна контролировать несанкционированное копирование важной информации (например, информация, являющаяся объектом интеллектуальной собственности) увольняемым персоналом и работающими по договору.

8.2 Классификация информации

Цель: Обеспечить надлежащий уровень защиты информации в соответствии с ее важностью для организации.

8.2.1 Основные принципы классификации информации

Средство управления

Классификация информации по требованиям законодательства, а также по важности, критичности и чувствительности для предотвращения ее несанкционированного разглашения или модификации.

Руководство по внедрению

При классификации информации и связанных с ней средств управления информационной безопасностью следует учитывать потребность бизнеса в совместном использовании или ограничении доступа к информации, а также требования законодательства. Другие активы, посредством которых информация хранится, обрабатывается либо используется иным способом, или защищается, можно также классифицировать в соответствии с классификацией этой информации.

Ответственными за классификацию информационных активов должны быть назначены их владельцы.

Система классификации информации должна включать соглашения о классификации и критерии пересмотра классификации с течением времени. Уровень защиты в системе классификации информации должен определяться посредством анализа конфиденциальности, целостности и доступности информации, а также с учетом любых других требований. Система классификации информации должна соответствовать политике управления доступом (9.1.1).

Каждому уровню должно быть присвоено имя, которое имеет смысл в контексте применяемой схемы классификации.

Утвержденная система классификации информации должна использоваться во всей организации, чтобы все классифицировали информацию и связанные с ней активы однообразно, одинаково понимали требования по защите и применяли соответствующую защиту.

Классификация должна быть включена в процессы организации, должна быть подходящей и понятной всему персоналу организации. Результаты классификации должны указывать на важность активов в зависимости от их чувствительности и критичности для организации, например, относительно конфиденциальности, целостности и доступности. Результаты классификации должны корректироваться при изменении важности, чувствительности и критичности активов в течение их жизненного цикла.

Дополнительная информация

Классификация позволяет людям, которые имеют дело с информацией, быстро определить, как обращаться с данной информацией и как защищать ее. Необходимо группировать информацию с учетом необходимого уровня ее защиты, это упростит определение процедур обеспечения информационной безопасности, которые будут относиться ко всей информации в каждой группе. Этот метод уменьшает потребность в определении рисков для каждого конкретного случая и при выполнении проекта средств управления по техническим условиям заказчика.

По истечении определенного периода времени информация может перестать быть чувствительной или критичной, например, после ее опубликования. Данные вопросы следует принимать во внимание, поскольку избыточная классификация может привести к реализации ненужных средств управления, что, в свою очередь, приведет к дополнительным расходам, или, наоборот, недостаточная классификация может поставить под угрозу достижение бизнес-целей.

Например, система классификации информации по уровню конфиденциальности может быть основана на четырех следующих уровнях, а именно что разглашение информации:

a) не причинит никакого вреда организации;

b) станет причиной незначительных затруднений или неудобств в деятельности организации;

c) окажет краткосрочное значительное влияние на операции или тактические цели организации;

d) окажет серьезное влияние на долгосрочные стратегические цели или станет причиной возникновения риска того, что организация окажется на грани выживания.

8.2.2 Маркировка информации

Средство управления

Разработка и внедрение соответствующего набора процедур по маркировке информации в соответствии с системой классификации, принятой в организации.

Руководство по внедрению

Процедуры по маркировке должны распространяться на информацию и связанные с ней активы, представленные как в физической, так и в электронной форме. Маркировка должна выполняться в соответствии с системой классификации, установленной в 8.2.1. Метки должны быть легко распознаваемы. Процедуры по маркировке должны определять, где и как должны быть расположены метки с учетом доступности информации или активов, обрабатываемых в зависимости от типов носителя. Для снижения рабочей нагрузки в процедурах по маркировке могут быть определены случаи, когда метка не ставится,

например, метка открытой информации. Служащие и работающие по договору должны быть осведомлены о процедурах по маркировке.

При осуществлении вывода данных из систем, содержащих информацию, которая классифицирована как чувствительная или критическая, следует использовать соответствующий гриф секретности.

Дополнительная информация

Маркировка классифицированной информации является ключевым требованием в соглашениях по совместному использованию информации. Обычной формой маркировки являются физические метки и метаданные.

Маркировка информации и связанных с ней активов иногда может иметь и отрицательный эффект. Классифицированные активы легче будет идентифицировать и, соответственно, украсть внутренним или внешним нарушителям.

8.2.3 Управление активами

Средство управления

Разработка и внедрение процедур управления активами в соответствии с системой классификации, принятой в организации.

Руководство по внедрению

Процедуры управления активами следует выполнять при обработке, хранении и передаче информации в соответствии с их классификацией (8.2.1).

При управлении активами должны быть учтены следующие вопросы:

a) ограничение доступа в соответствии с требованиями по защите, установленными для каждого уровня классификации;

b) сохранение надлежаще оформленных записей о полномочных получателях активов;

c) защита временных или постоянных копий информации в соответствии с уровнем защиты оригинала информации;

d) хранение активов ИТ в соответствии с требованиями изготовителей;

e) четкая маркировка всех копий носителя для привлечения внимания полномочного получателя.

Система классификации, используемая в организации, может не соответствовать системам, используемым в других организациях, даже если в них используются такие же названия уровней. Кроме того, классификации информации, которой обмениваются между собой организации, может изменяться в зависимости от ее контекста в каждой организации, даже если их системы классификации идентичны.

В соглашения с другими организациями, предусматривающие совместное использование информации, следует включать процедуры установления классификации данной информации и интерпретации меток классификации других организаций.

8.3 Обращение с носителями информации

Цель: Предотвратить несанкционированное разглашение, модификацию, удаление или уничтожение информации, хранимой на носителях информации.

8.3.1 Управление съемными носителями информации

Средство управления

Внедрение процедур по управлению съемными носителями в соответствии с системой классификации, принятой в организации.

Руководство по внедрению

При управлении съемными носителями должны быть учтены следующие рекомендации:

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

b) о носителях, выносимых за пределы организации, необходимо производить запись в постоянно хранимом регистрационном журнале, а также, где это необходимо и целесообразно, нужно применять их авторизацию;

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

d) если конфиденциальность или целостность данных являются важными факторами, которые необходимо учитывать, то для защиты данных на съемных носителях должны использоваться методы криптографической защиты;

e) для снижения риска порчи хранимых данных на носителе также необходимо, чтобы эти данные были перезаписаны на новый носитель прежде, чем они перестанут читаться;

f) многочисленные копии важных данных должны храниться на отдельных носителях, чтобы впоследствии уменьшить риск случайной порчи или потери данных;

g) следует рассмотреть вопрос регистрации съемных носителей для ограничения возможности потери данных;

h) установку дисководов съемных носителей следует разрешать только при служебной необходимости;

i) если необходимо использовать съемный носитель для передачи информации, то этот носитель следует проверить.

Процедуры и уровни авторизации должны быть документированы.

8.3.2 Утилизация носителей информации

Средство управления

Внедрение формальных процедур по надежной и безопасной утилизации носителей информации по окончании их использования.

Руководство по внедрению

Для минимизации риска разглашения конфиденциальной информации лицам, не имеющим к ней допуска, должны быть установлены формальные процедуры безопасной утилизации носителей информации. Процедуры безопасной утилизации носителей должны быть соразмерны чувствительности этой информации. При утилизации носителей информации должны быть учтены следующие вопросы:

a) носители, содержащие конфиденциальную информацию, следует хранить и утилизировать с соблюдением требований по безопасности, например, посредством сжигания либо измельчения, а в том случае, когда планируется эти носители использовать в пределах организации для других задач, то информация на них должна быть уничтожена;

b) следует внедрить процедуры определения носителей, для которых может потребоваться безопасная утилизация;

c) возможно, что все собранные носители информации будет проще утилизировать с соблюдением требований по безопасности, чем пытаться сортировать их по степени чувствительности;

d) многие организации предлагают услуги по сбору и утилизации носителей информации; следует проявлять осторожность при выборе подходящего подрядчика, имеющего необходимые средства управления и опыт;

e) следует регистрировать в журнале аудита факты утилизации носителей с чувствительной информацией.

При накоплении носителей для утилизации необходимо учитывать эффект агрегирования, в результате которого не чувствительная в разрозненном виде информация может стать чувствительной в том случае, если она была собрана в большом количестве.

Дополнительная информация

Для поврежденных устройств, содержащих чувствительные данные, может потребоваться определение рисков, чтобы принять решение, следует ли физически уничтожить эти устройства, отправить их в ремонт или списать (11.2.7).

8.3.3 Безопасность носителей информации при транспортировке

Средство управления

Защита носителей, содержащих информацию, во время транспортировки от несанкционированного доступа, неправомерного использования и повреждения.

Руководство по внедрению

Для защиты транспортируемых носителей информации должны быть учтены следующие рекомендации:

a) следует использовать надежных перевозчиков или курьеров;

b) список уполномоченных курьеров необходимо согласовывать с руководством;

c) следует разработать процедуры проверки идентификации курьеров;

d) упаковка носителей информации должна быть достаточной для защиты содержимого от любого физического повреждения, которое может иметь место при их транспортировке, и соответствовать требованиям изготовителей, защищая от воздействия любых факторов среды, например, от высокой температуры, влажности или электромагнитных полей, которые могут снизить эффективность восстановления носителей;

e) следует фиксировать в журнале описание содержимого носителя, применение защиты, а также записывать время передачи соответствующему курьеру и время вручения в пункте назначения.

Дополнительная 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. Это требование относится ко всем носителям информации, включая бумажные документы.

Если конфиденциальная информация на носителе не зашифрована, то следует обеспечить его дополнительную физическую защиту.

9 Управление доступом

9.1 Требования бизнеса при управлении доступом

Цель: Ограничить доступ к информации и средствам обработки информации.

9.1.1 Политика управления доступом

Средство управления

Определение, документирование и пересмотр политики управления доступом на основе требований бизнеса и требований информационной безопасности.

Руководство по внедрению

Владельцы актива должны определить соответствующие правила управления доступом, права доступа и ограничения для конкретных ролей пользователей к их активам с учетом подробного и точного описания

средств управления, предотвращающих риски информационной безопасности, связанные с доступом. Средства управления доступом являются как логическими, так и физическими (раздел 11), и их нужно рассматривать вместе. Пользователи и провайдеры услуг должны быть оповещены о необходимости выполнения требований бизнеса в части средств управления доступом.

В политике следует учитывать следующее:

a) требования по безопасности бизнес-приложений;

b) политики распространения и авторизации информации, например, принцип «положено знать» и уровни информационной безопасности, а также классификацию информации (7.2);

c) непротиворечивость между правами доступа и политиками классификации информации в системах и сетях;

d) существующее законодательство и любые договорные обязательства относительно ограничения доступа к данным или сервисам (18.1);

e) управление правами доступа в распределенной и сетевой среде с учетом всех типов доступных соединений;

f) разделение ролей, относящихся к управлению доступом, например, запрос на доступ, авторизация доступа, администрирование доступа;

g) требования к формальной авторизации запросов на доступ (9.2.1 и 9.2.2);

h) требования по периодическому пересмотру прав доступа (9.2.5);

i) изъятие прав доступа (9.2.6);

j) архивные записи о всех значимых событиях относительно использования и управления идентификаторами пользователей и секретной информацией аутентификации;

k) роли с привилегированным доступом (9.2.3).

Дополнительная информация

При определении правил управления доступом следует принимать во внимание следующее:

a) разработка правил основана на принципе «запрещено все, что явным образом не разрешено», а не на более слабом принципе «разрешено все, что явным образом не запрещено»;

b) изменения в маркировке информации (см. 7.2), которые инициируются автоматически средствами обработки информации и изменения, которые инициируются по усмотрению пользователя;

c) изменения в полномочиях пользователя, которые инициируются информационной системой и аналогичные изменения, которые инициируются администратором;

d) правила, которые требуют специального утверждения перед введением в действие, и правила, для которых этого не требуется.

Правила управления доступом следует поддерживать с помощью формальных процедур (9.2, 9.3, 9.4) и четко определенной ответственности (6.1.1, 9.3).

Управление доступом на основе ролей является методом, успешно используемым многими организациями и связывающим права доступа с бизнес-ролями.

К принципам, определяющим политику управления доступом, относятся два следующих часто встречающихся принципа:

a) «положено знать»: пользователю предоставляют доступ только к той информации, которая ему необходима для выполнения его задачи (для других задач/ролей «положено знать» означает другое и, следовательно, в этом случае будет указан другой профиль доступа);

b) «положено использовать»: пользователю предоставляют доступ только к тем средствам обработки информации (оборудованию ИТ, приложениям, процедурам, помещениям), которые ему необходимы для выполнения его задачи/работы/роли.

9.1.2 Доступ к сетям и сетевым сервисам

Средство управления

Предоставление непосредственного доступа пользователям к сетям и сетевым сервисам только при наличии соответствующих полномочий.

Руководство по внедрению

При формулировании политики использования сетей и сетевых сервисов должны быть определены:

a) сети и сетевые сервисы, к которым разрешен доступ;

b) процедуры авторизации, определяющие кому, к каким сетям и сетевым сервисам разрешен доступ;

c) административные средства управления и процедуры для защиты от несанкционированного доступа к сетевым сервисам;

d) средства, используемые для доступа к сетям и сетевым сервисам (например, использование виртуальных частных или беспроводных сетей);

e) требования к аутентификации пользователей для доступа к различным сетевым сервисам;

f) мониторинг использования сетевых сервисов. Политика использования сетевых сервисов не должна противоречить политике управления доступом организации (9.1.1).

Дополнительная информация

Несанкционированные и незащищенные подключения к сетевым сервисам могут повлиять на безопасность всей организации.

Управление доступом имеет особо важное значение для сетевых подключений к конфиденциальным или критически важным бизнес-приложениям, а также для пользователей, находящихся в местах повышенного риска (например, в общественных местах или за пределами

организации, то есть вне области действия управления информационной безопасностью и средств управления организации).

9.2 Управление доступом пользователей

Цель: Обеспечить санкционированный и предотвратить несанкционированный доступ пользователей к системам и сервисам.

9.2.1 Регистрация и разрегистрация пользователей

Средство управления

Внедрение формального процесса регистрации и разрегистрации пользователей, позволяющего назначать права доступа.

Руководство по внедрению

Процесс управления идентификаторами пользователей должен включать:

a) использование уникальных идентификаторов пользователей, позволяющих соотнести с каждым пользователем выполняемые им действия и возложить ответственность за эти действия на этого пользователя; использование общих идентификаторов допустимо только в том случае, если это необходимо для бизнеса или по эксплуатационным причинам, причем это должно быть санкционировано и задокументировано;

b) немедленную отмену или блокирование идентификаторов пользователей, которые уволились из организации (9.2.6);

c) периодическую проверку, удаление или блокирование идентификаторов и учетных записей уволенных пользователей;

d) проверку того, не выданы ли идентификаторы уволенных пользователей другим пользователям.

Дополнительная информация

Предоставление или отмена доступа к информации или средствам обработки информации является, как правило, двухступенчатой процедурой:

a) присвоение и задействование, либо отмена идентификатора пользователя;

b) предоставление или отмена прав доступа пользователю этого идентификатора (9.2.2).

9.2.2 Предоставление доступа пользователям

Средство управления

Внедрение формального процесса предоставления доступа пользователям, позволяющего предоставлять или отменять права доступа ко всем системам и сервисам пользователям всех типов.

Руководство по внедрению

Процесс предоставления доступа, необходимый для предоставления или отмены прав доступа пользователям, получивших идентификаторы, должен включать:

a) получение разрешения от владельца информационной системы или сервиса на их использование (8.1.2, средство управления); также может потребоваться отдельное подтверждение прав доступа со стороны руководства;

b) проверку того факта, что предоставленный уровень доступа соответствует как политикам доступа (9.1), так и другим требованиям, например, требованиям по разграничению обязанностей (6.1.2);

c) обеспечение гарантий того, что права доступа не будут активированы (например, провайдерами услуг) до завершения процедур авторизации;

d) поддержку системы централизованного учета прав доступа к информационным системам и сервисам, предоставленных пользователям идентификаторов;

e) приведение в соответствие прав доступа тех пользователей, у которых изменились роли или рабочие места, а также немедленное аннулирование или блокирование прав доступа уволенных пользователей;

f) периодический анализ прав доступа совместно с владельцами информационных систем или сервисов (9.2.5).

Дополнительная информация

Следует уделять внимание определению ролей для доступа пользователей, основанных на требованиях бизнеса и объединяющих целый ряд прав доступа в типовых профилях доступа. Запросы на доступ проверки доступа (9.2.4) легче администрировать на уровне подобных ролей, чем на уровне отдельных прав доступа.

Необходимо рассмотреть возможность включения в трудовые договора персонала и договора на оказание услуг положений о применении соответствующих санкций в случае попыток несанкционированного доступа, предпринятых сотрудником или работающим по договору (7.1.2, 7.2.3, 13.2.3, 15.1.2).

9.2.3 Управление привилегированными правами доступа

Средство управления

Ограничение и контроль предоставления и использования привилегированных прав доступа.

Руководство по внедрению

Предоставление привилегированных прав доступа должно контролироваться посредством формального процесса авторизации. При этом целесообразно применять следующие меры:

a) идентифицировать привилегированные права доступа, связанные с каждой системой или процессом, например, с операционной системой,

системой управления базами данных и каждым отдельным приложением, а также пользователей, которым эти привилегированные права доступа нужно предоставить;

b) привилегированные права доступа должны предоставляться пользователям только при наличии такой необходимости и для каждого конкретного случая в отдельности, в соответствии с политикой управления доступом (9.1.1), то есть уровень привилегий должен быть минимально возможным для функциональной роли пользователя;

c) необходимо обеспечивать процесс авторизации и регистрации всех предоставленных привилегий. Привилегированные права доступа не должны предоставляться до завершения процесса авторизации;

d) следует определить требования о прекращении действия привилегированных прав доступа;

e) следует использовать различные идентификаторы пользователей в повседневной бизнес-деятельности и при использовании привилегированных прав доступа. Осуществлять повседневную бизнес-деятельность, используя привилегированный идентификатор, запрещается;

f) компетентность пользователей с привилегированными правами доступа должна регулярно проверяться на предмет соответствия их своим обязанностям;

g) следует установить и поддерживать специфические процедуры для исключения возможности несанкционированного использования идентификаторов администраторов другими пользователями с учетом возможностей конфигурации систем;

h) при администрировании общих идентификаторов пользователей следует обеспечивать конфиденциальность секретной информации аутентификации в среде коллективного использования (например, обычно путем замены в максимально короткий срок пароля, когда привилегированный пользователь уходит в отпуск или меняет работу, рассылая его между привилегированными пользователями посредством соответствующих механизмов).

Дополнительная информация

Неправомерное использование привилегий системного администратора (функциональных возможностей или средств информационной системы, позволяющих пользователю блокировать средства управления системы или приложения) может быть главным фактором, способствующим сбоям или нарушениям защиты системы.

9.2.4 Управление секретной информацией аутентификации пользователей

Средство управления

Контроль предоставления секретной информации аутентификации посредством формального процесса управления.

Руководство по внедрению

Этот процесс должен отвечать следующим требованиям:

a) пользователям следует подписать соглашение о необходимости соблюдения полной конфиденциальности личной секретной информации аутентификации, а в отношении групповых паролей - соблюдения конфиденциальности в пределах рабочей группы. Данное подписанное соглашение может быть включено в условия трудового договора (7.1.2);

b) в тех случаях, когда пользователям требуется управление их собственной секретной информации аутентификации, необходимо обеспечивать предоставление безопасной первоначальной временной секретной информации аутентификации, которую пользователи обязаны сменить при первой регистрации в системе;

c) должны быть установлены процедуры подтверждения личности пользователя перед предоставлением ему новой, замененной или временной секретной информации аутентификации;

d) временную секретную информацию аутентификации следует предоставлять пользователям безопасным способом; следует избегать передачи паролей через посредников или посредством незащищенных (открытым текстом) сообщений электронной почты;

e) временная секретная информация аутентификации должна быть уникальной для каждого пользователя и не должна быть предсказуемой;

f) пользователям следует подтверждать получение секретной информации аутентификации;

g) секретная информация аутентификации, используемая изготовителями по умолчанию, должна быть заменена после установки систем или программного обеспечения.

Дополнительная информация

В большинстве случаев в качестве секретной информации аутентификации используются пароли, которые представляют собой обычное средство проверки личности пользователя. Существуют и другие виды секретной информации аутентификации, например, криптографические ключи и другие данные, хранимые на аппаратных токенах (например, на смарт-картах), которые генерируют коды аутентификации.

9.2.5 Пересмотр прав доступа пользователей

Средство управления

Регулярный пересмотр прав доступа пользователей владельцами активов.

Руководство по внедрению

При пересмотре прав доступа должно быть учтено следующее:

a) права доступа пользователей должны пересматриваться регулярно и после любых изменений, таких как повышение или понижение в должности, или прекращение трудового договора (раздел 7);

b) права доступа пользователей следует пересматривать и переназначать при переводе с одной роли на другую в пределах организации;

c) авторизация привилегированных прав доступа должна осуществляться через меньшие интервалы времени;

d) предоставленные привилегии должны периодически проверяться, чтобы обеспечить уверенность в том, что не были получены неавторизованные привилегии;

e) изменения в привилегированных учетных записях следует регистрировать для периодического контроля.

Дополнительная информация

Это средство управления компенсирует потенциальные слабости в реализации средств управления 9.2.1, 9.2.2 и 9.2.6.

9.2.6 Удаление или изменение прав доступа

Средство управления

Удаление или изменение прав доступа всего персонала и пользователей сторонних организаций к информации и средствам обработки информации при прекращении или изменении трудового договора, контракта или договора на оказание услуг.

Руководство по внедрению

При прекращении трудового договора, контракта или договора на оказание услуг права доступа отдельного лица к информации и активам, связанными с информацией, средствами обработки информации и сервисами, должны быть удалены или заблокированы. Эти события определяют необходимость удаления прав доступа. При переводе на другую должность у сотрудника должны быть удалены все те права доступа, которые не утверждены для этой должности. Удаление или изменение прав доступа распространяется как на физический, так и на логический доступ. Удаление или изменение прав доступа может быть выполнено посредством удаления, аннулирования или замены ключей, удостоверений личности или идентификационных карт, средств обработки информации или подписок. Удаление или изменение прав доступа должно быть отражено в любой документации, в которой определяются права доступа персонала и работающих по договору. Если увольняющийся сотрудник или пользователь сторонней организации знает пароли и действующие идентификаторы пользователя, эти пароли должны быть изменены при прекращении или изменении трудового договора, контракта или договора на оказании услуг.

Еще до прекращения или изменения трудового договора права доступа к информации и активам, связанным со средствами обработки информации, должны быть уменьшены или удалены в зависимости от оценки таких, например, факторов риска:

a) кем было инициировано прекращение или изменение трудового договора (сотрудником, пользователем сторонней организации или руководством организации) и причина прекращения трудового договора;

b) текущая ответственность сотрудника, пользователя сторонней организации или любого другого пользователя;

c) стоимость активов, доступных на настоящий момент.

Дополнительная информация

При определенных обстоятельствах распределение прав доступа основывается на доступности групповых идентификаторов большему количеству людей, чем увольняющийся сотрудник или пользователь сторонней организации. В данном случае увольняющиеся сотрудники должны быть удалены из любых групповых списков доступа и должно быть отдано распоряжение всему персоналу и пользователям сторонней организации о запрещении совместного использования этой информации с увольняющимся лицом.

В случае прекращения трудового договора по инициативе руководства организации недовольные сотрудники или пользователи сторонней организации могут умышленно исказить информацию или вывести из строя средства обработки информации. В случае же увольнения или освобождения от должности по собственному желанию, возможно, что эти лица захотят собрать информацию, чтобы впоследствии ее использовать.

9.3 Ответственность пользователей

Цель: Возложить на пользователей ответственность за сохранность их информации аутентификации.

9.3.1 Использование секретной информации аутентификации

Средство управления

Требование к пользователям о соблюдении правил организации в части использования секретной информации аутентификации.

Руководство по внедрению

Все пользователи должны быть осведомлены о:

a) необходимости сохранения конфиденциальности секретной информации аутентификации, обеспечения ее неразглашения любым другим сторонам, включая представителей уполномоченных органов;

b) недопустимости записи секретной информации аутентификации (например, на бумаге, в программные файлы или карманные устройства), если невозможно обеспечить ее безопасное хранение и если метод хранения не утвержден;

c) необходимости изменения секретной информации аутентификации каждый раз, когда появляются признаки ее возможной компрометации;

d) том, что если в качестве секретной информации аутентификации используются пароли, то следует выбирать качественные пароли с достаточной минимальной длиной, которые:

1) легко запомнить;

2) не основаны на чем-либо, что можно легко угадать или выяснить, используя персональные данные владельца пароля, например, имя, номера телефонов, дату рождения и т. д.;

3) не уязвимы к атаке по словарю (то есть не состоят из слов, включенных в словари);

4) не содержат последовательностей одинаковых символов, не состоят только из цифр или только из букв;

5) заменят временные пароли при первой регистрации в системе;

e) недопустимости использования индивидуальной секретной информации аутентификации пользователя совместно с кем-либо;

f) необходимости обеспечения соответствующей защиты паролей, если они используются и хранятся в качестве секретной информации аутентификации для процедур автоматической регистрации;

g) том, что не следует использовать один и тот же пароль в служебных и неслужебных целях.

Дополнительная информация

Использование средств единого безопасного доступа на основе технологии однократной аутентификации (Single Sign On, SSO) или других инструментальных средств управления секретной информацией аутентификации снижает объем секретной информации аутентификации (например, количество паролей), которую необходимо знать пользователям, может повысить эффективность вышеуказанного средства управления. Однако, использование этих инструментальных средств может также повысить возможность раскрытия секретной информации аутентификации.

9.4 Управление доступом к системе и приложениям

Цель: Предотвратить несанкционированный доступ к системам и приложениям.

9.4.1 Ограничение доступа к информации

Средство управления

Ограничение доступа к информации и функциям прикладных систем в соответствии с политикой управления доступом.

Руководство по внедрению

Ограничение доступа должно быть основано на индивидуальных требованиях бизнес-приложений и определенной политике управления доступом.

Для обеспечения требований по ограничению доступа необходимо принять во внимание следующее:

a) создание меню для управления доступом к функциям прикладной системы;

b) управление какими данными может быть доступно конкретному пользователю;

c) управление правами доступа пользователей, например, чтение, запись, удаление и выполнение;

d) управление правами доступа к другим приложениям;

e) ограничение информации, содержащейся в выходных данных;

f) обеспечение физического и логического управления доступом для отделения чувствительных приложений, прикладных данных или систем.

9.4.2 Безопасные процедуры входа в систему

Средство управления

Выполнение управления доступом к системам и приложениям посредством безопасной процедуры входа в систему в тех случаях, когда этого требует политика управления доступом.

Руководство по внедрению

Для подтверждения предъявленной идентификационной информации пользователя должен быть выбран соответствующий метод аутентификации. В тех случаях, когда требуется сильная аутентификация и верификация идентификационной информации, наряду с паролями должны использоваться альтернативные методы аутентификации, например, криптографические средства, смарт-карты, токены или биометрические средства.

Процедура входа в систему или приложение должна быть разработана таким образом, чтобы свести к минимуму возможность несанкционированного доступа. Следовательно, процедура входа в систему должна сообщать минимум информации о системе или приложении, чтобы не предоставлять излишнюю поддержку неавторизованному пользователю. Правильно спланированная процедура входа в систему должна удовлетворять следующим требованиям:

a) не отображать на экране идентификаторы системы или приложений до успешного завершения процесса входа в систему;

b) выводить на экран общее уведомление, предупреждающее, что доступ к компьютеру могут получить только авторизованные пользователи;

c) во время процесса входа в систему не выводить на экран справочные сообщения, которые могут помочь неавторизованному пользователю;

d) подтверждать правильность регистрационной информации только после завершения ввода всех данных. При возникновении ошибки система не должна указывать, какая часть данных является правильной или неправильной;

e) защищать от грубых попыток принудительного входа в систему;

f) регистрировать неудачные и успешные попытки;

g) уведомлять о событии информационной безопасности при обнаружении потенциальной попытки или успешного обхода средств управления входом в систему;

h) при успешном выполнении входа в систему отображать следующую информацию:

1) дата и время последнего успешного входа в систему;

2) сведения о неудачных попытках входа в систему с момента последнего успешного входа в систему;

i) не отображать на экране вводимый пароль;

j) не передавать пароли по сети открытым текстом;

k) завершать неактивные сеансы после определенного периода неактивности, особенно в местоположениях высокого риска, например, в общественных местах или местах, находящихся за пределами территории организации, или на мобильных устройствах;

l) ограничивать время соединения с целью обеспечения дополнительной безопасности для приложений высокого риска и уменьшения окна возможности для несанкционированного доступа.

Дополнительная информация

Если во время входа в систему пароли передаются по сети открытым текстом, то они могут быть перехвачены в сети программой сетевого анализатора трафика («сниффером»).

9.4.3 Система управления паролями

Средство управления

Использование интерактивных систем управления паролями, обеспечивающих качество паролей.

Руководство по внедрению

Система управления паролями должна:

a) обязывать пользователей использовать индивидуальные идентификаторы и пароли для обеспечения подотчетности;

b) позволять пользователям выбирать и изменять свои пароли, а также включать процедуру подтверждения, предохраняющую от ошибок при вводе;

c) обеспечивать выбор надежных паролей;

d) обязывать пользователей менять временные пароли при первом входе в систему;

e) обязывать регулярно менять пароль и при необходимости;

f) хранить сведения о ранее использовавшихся паролях пользователей и предотвращать их повторное использование;

g) не отображать пароли на экране при их вводе;

h) хранить файлы паролей отдельно от данных прикладной системы;

i) хранить и передавать пароли в защищенной (например, зашифрованной или хэшированной) форме.

Дополнительная информация

Для некоторых бизнес-приложений требуется назначение паролей пользователей независимым должностным лицом; в таких случаях приведенные выше перечисления b), d) и e) не применяются. В большинстве случаев пароли выбираются и поддерживаются самими пользователями.

9.4.4 Использование привилегированных программных утилит

Средство управления

Ограничение и строгий контроль использования программных утилит (служебных программ), способных обходить системные и прикладные средства управления.

Руководство по внедрению

Необходимо выполнение следующих рекомендаций по использованию программных утилит, способных обходить системные и прикладные средства управления:

a) использование для программных утилит процедур идентификации, аутентификации и авторизации;

b) отделение программных утилит от прикладного программного обеспечения;

c) ограничение использования программных утилит минимально возможным количеством доверенных авторизованных пользователей, которым это необходимо (9.2.3);

d) авторизация использования программных утилит для каждого конкретного случая;

e) ограничение доступности программных утилит, например, только на время внесения авторизованных изменений;

f) регистрация всех случаев использования программных утилит;

g) определение и документирование уровней авторизации для программных утилит;

h) удаление или отключение всех ненужных программных утилит;

i) недоступность программных утилит для пользователей, имеющих доступ к приложениям в тех системах, в которых требуется разделение обязанностей.

Дополнительная информация

В большинстве компьютеров имеется одна или несколько программных утилит, которые способны обходить системные и прикладные средства управления.

9.4.5 Управление доступом к исходным кодам программ

Средство управления

Ограничение доступа к исходным кодам программ.

Руководство по внедрению

Доступ к исходным кодам программ и связанной с ними документации (например, к проектам, спецификациям, планам экспертизы программного обеспечения) необходимо строго контролировать, чтобы предотвратить введение несанкционированных функциональных возможностей и избежать непреднамеренных изменений, а также поддерживать конфиденциальность ценной интеллектуальной собственности. Этих целей для исходных кодов программ можно достичь с помощью контролируемого центрального запоминающего устройства этих кодов, предпочтительно в библиотеках исходного кода программ. Для снижения вероятности повреждения компьютерных программ необходимо принять во внимание следующие рекомендации по управлению доступом к библиотекам исходных кодов программ:

a) по возможности, библиотеки исходного кода программ не должны содержаться в действующих системах;

b) управление исходным кодом программ и библиотеками исходного кода программ должно осуществляться в соответствии с установленными процедурами;

c) персонал службы технической поддержки не должен иметь неограниченного доступа к библиотекам исходного кода программ;

d) обновление библиотек исходного кода программ и связанной с ними документации, а также предоставление исходных кодов программистам, должно осуществляться только после получения соответствующего разрешения;

e) листинги программ должны храниться в безопасной среде;

f) необходимо вести журнал аудита для регистрации всех случаев доступа к библиотекам исходного кода программ;

g) техническая поддержка и копирование библиотек исходного кода программ должны выполняться в строгом соответствии с процедурами контроля над внесением изменений (14.2.2).

Если исходный код программ предполагается опубликовать, то следует принять во внимание дополнительные средства управления (например, электронную цифровую подпись), которые помогут удостовериться в его целостности.

10 Криптографическая защита информации

10.1 Средства криптографической защиты информации

Цель: Обеспечить правильное и эффективное использование средств криптографической защиты информации для защиты конфиденциальности, аутентичности и/или целостности информации.

10.1.1 Политика использования средств криптографической защиты информации

Средство управления

Разработка и внедрение политики использования средств криптографической защиты информации.

Руководство по внедрению

При разработке политики использования средств криптографической защиты информации необходимо учитывать следующее:

a) подход руководства к применению средств криптографической защиты информации в организации, включая общие принципы защиты бизнес-информации;

b) требуемый уровень защиты, основанный на определении рисков, с учетом типа, стойкости и качества требуемого алгоритма шифрования;

c) использование шифрования для защиты конфиденциальной информации, передаваемой на мобильных или сменных носителях, устройствах, либо по линиям телекоммуникаций;

d) подход к управлению ключами, включая методы обеспечения защиты криптографических ключей и восстановления зашифрованной информации в случае утраты, компрометации или повреждения ключей;

e) распределение ролей и ответственности должностных лиц, ответственных за:

1) реализацию политики;

2) управление ключами, в том числе генерацию ключей (10.1.2);

f) стандарты, которые должны быть приняты для эффективного внедрения во всей организации (какие именно решения используются для данных бизнес-процессов);

g) влияние используемого шифрования информации на средства управления, которые зависят от контроля содержимого (например, обнаружение вредоносных программ).

При внедрении политики использования средств криптографической защиты информации в организации следует учитывать требования национального законодательства и ограничения, которые могут применяться в отношении использования криптографических методов, а также вопросы, связанные с передачей потоков информации за пределы страны (18.1.5).

Средства криптографической защиты информации можно использовать для достижения различных целей безопасности, например, таких как:

a) конфиденциальность: использование шифрования информации для защиты чувствительной или критичной информации как при ее хранении, так и при передаче;

b) целостность/аутентичность: использование электронных цифровых подписей или кодов аутентификации сообщения для проверки аутентичности и целостности хранимой или передаваемой чувствительной или критичной информации;

c) неотказуемость: использование криптографических методов для получения свидетельств о наличии или отсутствии события или действия;

d) аутентификация: использование криптографических методов для отождествления пользователей и других системных логических объектов, запрашивающих доступ к пользователям, логическим объектам и ресурсам системы или взаимодействующих с ними.

Дополнительная информация

Принятие решения относительно применения криптографической защиты следует рассматривать как составную часть более общего процесса определения рисков и выбора средств управления. Определение рисков используется для независимого определения целесообразности применения средств криптографической защиты информации, а также для определения того, какое именно средство следует применять для данных целей и бизнес-процессов.

Политика использования средств криптографической защиты информации необходима для получения максимума преимуществ и минимизации рисков использования криптографических методов, а также для исключения их неправомерного или неправильного использования.

Для достижения целей политики информационной безопасности следует воспользоваться рекомендациями специалистов при выборе подходящих средств криптографической защиты информации.

10.1.2 Управление ключами

Средство управления

Разработка политики использования, защиты и жизненного цикла криптографических ключей и ее реализация в течение всего их жизненного цикла.

Руководство по внедрению

Политика должна включать требования по управлению криптографическими ключами в течение всего их жизненного цикла, в том числе требования по генерации, хранению, архивированию, восстановлению, распределению, изъятию из обращения и уничтожению ключей.

Криптографические алгоритмы, длину ключей и методы их использования следует выбирать с учетом передового опыта. Для

соответствующего управления ключами необходимы безопасные процессы генерации, хранения, архивирования, восстановления, распределения, изъятия из обращения и уничтожения криптографических ключей.

Все криптографические ключи должны быть защищены от модификации и потери. Кроме того, секретные и личные ключи нуждаются в защите от несанкционированного раскрытия. Оборудование, используемое для изготовления, хранения и архивирования ключей, должно быть физически защищено.

Система управления криптографическими ключами должна быть основана на согласованном наборе стандартов, процедур и безопасных методов, которые обеспечивают:

a) генерацию ключей при использовании различных криптографических систем и различных приложений;

b) выдачу и получение сертификатов открытых ключей;

c) распространение ключей среди предназначенных логических объектов, включая инструкции по их активации при получении;

d) хранение ключей, в том числе порядок получения доступа к ключам для авторизованных пользователей;

e) смену или обновление ключей, в том числе правила относительно порядка и сроков смены ключей;

f) порядок действий в отношении скомпрометированных ключей;

g) аннулирование ключей, в том числе порядок отзыва или деактивации ключей в том случае, например, если ключи были скомпрометированы или если соответствующий пользователь уволился из организации (в этом случае ключи также необходимо архивировать);

h) восстановление ключей, которые были утеряны или испорчены;

i) резервное копирование или архивирование ключей;

j) уничтожение ключей;

k) регистрация и аудит деятельности, связанной с управлением ключами.

Для уменьшения вероятности ненадлежащего использования ключей следует определить даты их активации и деактивации, чтобы эти ключи можно было использовать только в течение определенного периода времени в соответствии с политикой управления ключами.

Кроме безопасного управления секретными и личными ключами также следует рассмотреть вопрос об аутентификации открытых ключей. Данный процесс аутентификации можно выполнять с помощью сертификата открытых ключей, обычно выдаваемого центром сертификации, который должен быть официально признанной организацией, обладающей необходимыми средствами управления и процедурами для обеспечения требуемой степени доверия.

В соглашениях или контрактах об уровне предоставляемого обслуживания с внешними поставщиками (провайдерами) криптографических услуг, например, с центром сертификации, должны быть отражены

вопросы об ответственности, надежности обслуживания и времени предоставления запрашиваемых услуг (15.2).

Дополнительная информация

Управление криптографическими ключами является основным условием эффективного использования криптографических методов.

Криптографические методы могут также применяться и для защиты криптографических ключей. Может потребоваться разработка процедур для законодательно обоснованного доступа к криптографическим ключам, например, для расшифровки информации, используемой в качестве доказательства в суде.

11 Физическая безопасность и безопасность окружающей среды

11.1 Охраняемые зоны

Цель: Предотвратить несанкционированный физический доступ на территорию организации, повреждение информации и средств обработки информации, а также другие воздействия на них.

11.1.1 Физический периметр безопасности

Средство управления

Определение и использование периметров безопасности для защиты зон, в которых содержится чувствительная или критичная информация и средства обработки информации.

Руководство по внедрению

При необходимости, следует учесть и внедрить следующие рекомендации по оборудованию физического периметра безопасности:

a) периметры безопасности должны быть четко определены; расположение и надежность каждого из периметров должны зависеть от требований по безопасности активов, находящихся внутри периметра, и результатов определения рисков;

b) периметр здания или помещений, где расположены средства обработки информации, должен быть физически сплошным (то есть в периметре не должно быть никаких промежутков или мест, через которые можно было бы легко проникнуть). Крыша, внешние стены и полы помещений должны иметь достаточно прочную конструкцию, а все внешние двери должны быть соответствующим образом защищены от несанкционированного доступа с помощью устройств контроля доступа (например, турникетов, тревожной сигнализации, замков). В отсутствии персонала двери и окна должны закрываться на замок, для окон (особенно расположенных на первом этаже) следует рассмотреть вопрос о наружной защите;

c) необходимо создать контрольно-пропускной пункт с охраной или обеспечить другие способы управления физическим доступом на территорию или в здание; доступ на территорию или в здания должен предоставляться только тому персоналу, который имеет соответствующие полномочия;

d) при необходимости, для предотвращения несанкционированного физического доступа и загрязнения окружающей среды следует построить физические барьеры;

e) все запасные выходы и стены по периметру безопасности следует оборудовать аварийной сигнализацией и средствами наблюдения, с помощью которых необходимо контролировать и проверять обеспечение требуемого уровня защиты в соответствии с региональными, национальными и международными стандартами; оборудование запасных выходов должно соответствовать правилам пожарной безопасности и обладать отказоустойчивостью;

f) для охраны всех внешних дверей и легкодоступных окон следует установить и регулярно проверять системы обнаружения вторжения нарушителей, соответствующие государственным стандартам. В безлюдных охраняемых зонах должна быть круглосуточно включена сигнализация, также следует обеспечить охрану других зон, например, помещений с компьютерами или со средствами телекоммуникаций;

g) средства обработки информации, управляемые организацией, следует физически отделить от средств обработки информации, управляемых сторонней организацией.

Дополнительная информация

Физическая защита обеспечивается путем создания одного или более физических барьеров вокруг территории организации и помещений со средствами обработки информации. Использование нескольких барьеров обеспечивает дополнительную защиту, поскольку нарушение одного барьера не означает немедленную компрометацию системы безопасности.

Охраняемой зоной может быть запираемое помещение или несколько помещений, окруженных непрерывным внутренним барьером физической безопасности. Могут потребоваться дополнительные барьеры и периметры для управления физическим доступом между зонами внутри периметра безопасности, к которым предъявляются различные требования по безопасности. В том случае, когда активы нескольких организаций находятся в одном здании, следует уделять особое внимание безопасности физического доступа.

Применение физических средств управления, особенно для охраняемых зон, должно осуществляться в соответствии с техническими и экономическими возможностями организации, изложенными в определении рисков.

11.1.2 Средства управления физическим доступом

Средство управления

Защита охраняемых зон с помощью соответствующих средств управления доступом, позволяющих обеспечивать доступ только авторизованному персоналу, который имеет соответствующие полномочия.

Руководство по внедрению

Необходимо принять во внимание следующие рекомендации:

a) дата и время прихода/ухода посетителей должны регистрироваться; если доступ посетителей не был предварительно утвержден, их должны сопровождать должностные лица принимающего подразделения; посетителям доступ должен предоставляться только в конкретных, санкционированных целях, также они должны пройти инструктаж по требованиям по безопасности в данной зоне и действиям в чрезвычайных ситуациях. В качестве идентификаторов личности посетителей следует использовать соответствующие средства;

b) доступ к зонам, в которых обрабатывается или хранится конфиденциальная информация, должен ограничиваться только имеющими соответствующие полномочия лицами путем внедрения соответствующих средств управления доступом, например, таких механизмов двухфакторной аутентификации как карты доступа и секретный персональный идентификационный номер (personal identification number, PIN);

c) необходимо вести и регулярно просматривать прошнурованный журнал регистрации посетителей или защищенный электронный журнал регистрации событий, в которых должны регистрироваться все имевшие место случаи доступа;

d) весь персонал, а также все работающие по договору, пользователи сторонних организаций и все посетители в обязательном порядке должны иметь какие-либо видимые идентификационные знаки и немедленно уведомлять персонал службы безопасности, если они встретят посетителей без сопровождения или лиц, у которых отсутствует видимый идентификационный знак;

e) стороннему обслуживающему персоналу следует предоставлять ограниченный доступ в охраняемые зоны или к средствам обработки конфиденциальной информации только при необходимости; такой доступ должен быть санкционированным и постоянно контролируемым;

f) права доступа к охраняемым зонам следует регулярно пересматривать, обновлять, а при необходимости - аннулировать (9.2.5 и 9.2.6).

11.1.3 Безопасность зданий, производственных помещений и оборудования

Средство управления

Разработка и внедрение физической защиты для зданий, производственных помещений и оборудования.

Руководство по внедрению

Для защиты зданий, производственных помещений и оборудования следует принять во внимание следующие рекомендации:

a) основное оборудование должно быть расположено в местах с ограниченным доступом;

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

c) оборудование должно быть расположено таким образом, чтобы исключить возможность извне увидеть или услышать конфиденциальную информацию или деятельность. При необходимости следует применять электромагнитное экранирование;

d) адресные справочники и внутренние телефонные книги, указывающие на местонахождение средств обработки конфиденциальной информации, не должны находиться в свободном доступе для посторонних лиц.

11.1.4 Защита от внешних угроз и угроз окружающей среды

Средство управления

Разработка и внедрение физической защиты от стихийных бедствий, злонамеренных воздействий или чрезвычайных ситуаций.

Руководство по внедрению

Следует проконсультироваться со специалистами относительно того, как избежать ущерба от пожара, наводнения, землетрясения, взрыва, уличных беспорядков и других чрезвычайных ситуаций.

11.1.5 Выполнение работ в охраняемых зонах

Средство управления

Разработка и внедрение процедур работы в охраняемых зонах.

Руководство по внедрению

Необходимо принять во внимание следующие рекомендации:

a) о наличии охраняемой зоны и проводимых в ней работах должны быть осведомлены только те лица, которым это необходимо в силу производственной необходимости;

b) из соображений безопасности и предотвращения возможности злонамеренных действий в охраняемых зонах следует исключить возможность работы без наблюдения;

c) не используемые охраняемые зоны необходимо физически заблокировать и периодически проверять;

d) использование фото-, видео-, аудио- или другого записывающего оборудования, такого как камеры в мобильных телефонах, без специального разрешения не допускается.

Мероприятия по организации работы в охраняемых зонах включают использование средств контроля за работающими в охраняемой зоне персоналом и пользователями сторонних организаций, которые отслеживают всю деятельность, происходящую в охраняемой зоне.

11.1.6 Изолирование зон приемки и отгрузки материальных ценностей

Средство управления

Контроль зон приемки и отгрузки материальных ценностей, а также других мест, из которых можно проникнуть в помещения, и, при возможности, изолирование их от средств обработки информации во избежание несанкционированного доступа.

Руководство по внедрению

Необходимо принять во внимание следующие рекомендации:

a) доступ к зоне приемки и отгрузки материальных ценностей снаружи здания должен быть ограничен строго определенным персоналом, имеющим допуск;

b) зона приемки и отгрузки материальных ценностей должна быть спроектирована таким образом, чтобы персонал мог разгружать доставленный груз, не получая доступа к другим частям здания;

c) наружные двери зоны приемки и отгрузки материальных ценностей должны запираться при открытии внутренней двери;

d) поступающие материальные ценности должны быть тщательно осмотрены и проверены на наличие взрывоопасных и химических веществ или других опасных материалов, прежде, чем они будут перемещены из зоны приемки и отгрузки к местам использования;

e) поступающие материальные ценности должны быть зарегистрированы в соответствии с процедурами управления активами (раздел 8) при поступлении на территорию;

f) при наличии возможности следует физически разделять поступающие и исходящие материальные ценности;

g) поступающие материальные ценности должны быть тщательно осмотрены на предмет наличия признаков преднамеренного ущерба, полученного в пути следования. При обнаружении таких признаков следует немедленно сообщить об этом персоналу службы безопасности.

11.2 Безопасность оборудования

Цель: Предотвратить утрату, повреждение, хищение или компрометацию активов и нарушение непрерывного функционирования организации.

11.2.1 Размещение и защита оборудования

Средство управления

Размещение и защита оборудования таким образом, который позволит снизить риски, связанные с угрозами окружающей среды и стихийными бедствиями, а также с возможностью несанкционированного доступа.

Руководство по внедрению

Для защиты оборудования необходимо принять во внимание следующие рекомендации:

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

b) средства обработки информации с чувствительными данными следует размещать самым тщательным образом, чтобы уменьшить риск просмотра информации неавторизованными лицами во время ее использования;

c) средства хранения данных должны быть защищены от несанкционированного доступа;

d) объекты, требующие особой защиты, должны охраняться для снижения общего уровня необходимой защиты;

e) следует принять меры для минимизации риска потенциальных физических и внешних угроз окружающей среды, например, хищения, пожара, взрывов, задымления, затопления (или прекращения подачи воды), воздействия пыли, вибрации и химических веществ, помех в сети электропитания, взаимных помех средств телекоммуникаций, электромагнитного излучения и вандализма;

f) следует определить и утвердить свою политику относительно приема пищи, напитков и курения вблизи средств обработки информации;

g) следует постоянно вести мониторинг состояния окружающей среды, например, температуры и влажности, которые могут неблагоприятно повлиять на функционирование средств обработки информации;

h) следует на всех зданиях использовать молниеотводы, а на все входящие силовые линии и линии телекоммуникаций следует установить молниезащитные фильтры;

i) для оборудования, эксплуатируемого в производственной среде, следует использовать специальные средства защиты оборудования, например, защитные пленки для клавиатуры;

j) для минимизации риска утечки информации по каналам побочных электромагнитных излучений следует защищать оборудование, обрабатывающее конфиденциальную информацию.

11.2.2 Оборудование вспомогательных служб

Средство управления

Защита оборудования от перебоев в подаче электроэнергии и других нарушений, вызванных авариями оборудования вспомогательных служб.

Руководство по внедрению

Оборудование вспомогательных служб (например, служб электроснабжения, телекоммуникаций, водоснабжения, газоснабжения, канализации, вентиляции и кондиционирования воздуха) должно:

a) соответствовать техническим условиям изготовителя оборудования и требованиям национального законодательства;

b) периодически оцениваться на предмет его возможности удовлетворять потребности развивающегося бизнеса и взаимодействия с другими вспомогательными службами;

c) регулярно обследоваться и подвергаться соответствующим испытаниям, чтобы обеспечить его исправное функционирование;

d) при необходимости, установить системы оповещения для обнаружения нарушения его работоспособности;

e) при необходимости, подключаться к нескольким линиям электроснабжения, проложенным по разным трассам.

Следует предусмотреть аварийное освещение и аварийную связь. Аварийные выключатели и вентили для отключения в случае аварии электроснабжения, водоснабжения, газоснабжения или других вспомогательных служб должны быть расположены вблизи от запасных выходов или помещений с оборудованием.

Дополнительная информация

Дополнительная избыточность сетевого подключения может быть получена посредством множественных маршрутов к нескольким поставщикам коммунальных услуг.

11.2.3 Безопасность кабелей

Средство управления

Защита силовых кабелей и кабелей телекоммуникаций, по которым передаются данные или предоставляются дополнительные информационные сервисы, от перехвата информации, взаимных помех или повреждения.

Руководство по внедрению

Для обеспечения безопасности кабелей необходимо принять во внимание следующие рекомендации:

a) силовые кабели и линии телекоммуникаций, подключенные к средствам обработки информации, должны быть, по возможности, проложены под землей или защищены другими соответствующими альтернативными методами;

b) силовые кабели следует прокладывать отдельно от кабелей телекоммуникаций для исключения возникновения помех;

c) для систем с чувствительной или критической информацией следует предусмотреть дополнительные средства управления, к которым относятся:

1) использование армированных кабелепроводов, а также закрытие на замок помещений или шкафов промежуточных контрольных и конечных пунктов;

2) использование электромагнитного экранирования для защиты кабелей;

3) организация технического зондирования и физического обследования на предмет подключения несанкционированных устройств к кабелям;

4) контролируемый доступ к коммутационным панелям и кабельным шкафам.

11.2.4 Техническое обслуживание оборудования

Средство управления

Проведение надлежащего технического обслуживания оборудования для обеспечения его постоянной готовности и целостности.

Руководство по внедрению

При выполнении технического обслуживания оборудования следует принять во внимание следующие рекомендации:

a) оборудование следует обслуживать в соответствии с периодичностью, рекомендованной его изготовителем, и инструкциями по эксплуатации;

b) техническое обслуживание и ремонт оборудования должен выполнять только персонал, имеющий соответствующие полномочия;

c) необходимо регистрировать все предполагаемые или фактические неисправности, а также все виды профилактического и восстановительного технического обслуживания;

d) следует применять соответствующие средства управления с учетом того, где выполняется обслуживание персоналом: на месте или за пределами организации; при необходимости, следует удалять из оборудования конфиденциальную информацию, либо обслуживающий персонал должен иметь допуск к конфиденциальной информации достаточного уровня;

e) после завершения технического обслуживания и до начала штатной эксплуатации оборудования его следует проверить, чтобы убедиться в том, что данное оборудование полностью исправно и не будет работать со сбоями;

11.2.5 Вынос активов

Средство управления

Вынос оборудования, носителей с информацией или программным обеспечением из помещений организации только при наличии соответствующего разрешения.

Руководство по внедрению

Следует принять во внимание следующие рекомендации:

a) следует четко определить персонал и пользователей сторонних организаций, имеющих полномочия для выдачи разрешений на вынос активов за пределы организации;

b) следует установить предельный срок, на который выносятся активы, а при их возврате следует проверять соблюдение этого срока;

c) если это необходимо и целесообразно, то следует регистрировать как вынос активов за пределы организации, так и их возвращение;

d) следует задокументировать идентификатор, роль и принадлежность к организации каждого из тех, кто выносит или использует активы; этот документ возвращается вместе с оборудованием, информацией или программным обеспечением.

Дополнительная информация

Для обнаружения неразрешенных записывающих устройств, оружия и т. п., а также для предотвращения их попадания на территорию и выноса с территории организации могут также выполняться выборочные проверки, предпринимаемые для выявления несанкционированного выноса активов. Такие выборочные проверки следует проводить в соответствии с законодательными и нормативно-правовыми актами. Сотрудников следует предупредить о проведении выборочных проверок, проверки должны выполняться только при наличии санкций, удовлетворяющих требованиям законодательных и нормативно-правовых актов.

11.2.6 Безопасность оборудования и активов за пределами организации

Средство управления

Обеспечение безопасности активов, находящихся за пределами организации, с учетом различных рисков, связанных с работой вне организации.

Руководство по внедрению

Использование любого оборудования для хранения и обработки информации за пределами организации должно быть санкционировано руководством. Это требование относится как к оборудованию, принадлежащему организации, так и к личному оборудованию, используемому в интересах организации.

Для защиты оборудования за пределами организации следует принять во внимание следующие рекомендации:

a) оборудование и носители информации, вынесенные с территории организации, не следует оставлять без присмотра в общественных местах;

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

c) при нахождении за пределами организации, например, при работе на дому, дистанционной работе и работе на временных местах, следует посредством определения рисков определить и использовать при необходимости соответствующие средства управления, например, запираемые на замок шкафы для хранения документов, соблюдение политики «чистого стола», средства управления доступом к компьютеру и защищенную связь с офисом (см. также O‘z DSt ISO/IEC 27033-1, O‘z DSt ISO/IEC 27033-2, O‘z DSt ISO/IEC 27033-3, O‘z DSt ISO/IEC 27033-4, O‘z DSt ISO/IEC 27033-5);

d) в том случае, когда оборудование, находящееся за пределами организации, передается от одного лица или сторонней организации другому лицу или сторонней организации, факт передачи этого оборудования следует зафиксировать в соответствующем журнале; эта запись, включая название организации и данные лиц, ответственных за оборудование, будет служить доказательством смены ответственности за защиту данного оборудования.

Риски, связанные, например, с повреждением, воровством и прослушиванием, могут в значительной степени различаться в разных местах и должны приниматься в расчет при определении наиболее целесообразных средств управления.

Дополнительная информация

К оборудованию для хранения и обработки информации относятся все виды персональных компьютеров, органайзеры, мобильные телефоны, смарт-карты, а также бумажная документация и другие виды носителей данных, которые сотрудники забирают для работы на дому или увозят с обычного места работы.

Более подробная информация о других аспектах защиты мобильного оборудования приведена в 6.2.

Возможно, что во избежание рисков будет целесообразно запретить определенным сотрудникам работать за пределами организации или ограничить использование ими портативных и мобильных устройств.

11.2.7 Безопасная утилизация или повторное использование оборудования

Средство управления

Проверка и получение уверенности в том, что все чувствительные данные и лицензионное программное обеспечение были удалены или надежно перезаписаны до утилизации каждой единицы оборудования, содержащей запоминающие устройства.

Руководство по внедрению

До утилизации или повторного использования оборудования оно должно быть проверено, чтобы убедиться в том, содержатся ли в нем или отсутствуют запоминающие устройства.

Запоминающие устройства, содержащие конфиденциальную или охраняемую авторским правом информацию, следует физически уничтожать либо уничтожать, удалять или переписывать эту информацию, используя методы, которые не позволят восстановить исходную информацию, а не использовать стандартные функции удаления информации и форматирования диска.

Дополнительная информация

Для поврежденного оборудования, содержащего запоминающие устройства, может потребоваться определение рисков, чтобы определить, следует ли физически уничтожить это оборудование, отправить его в ремонт или вывести из эксплуатации. Из-за небрежной утилизации и повторного использования оборудования информация может быть скомпрометирована.

Риск раскрытия конфиденциальной информации при передаче оборудования на другой объект или продаже уменьшается как при использовании безопасной очистки диска, так и при шифровании всего пространства диска, при условии, что:

a) процесс шифрования достаточно долгий и охватывает весь диск (в том числе неиспользуемое пространство, файлы подкачки и т. п.);

b) криптографические ключи достаточно длинные, это позволяет противостоять атаке методом подбора ключа;

c) обеспечивается конфиденциальность криптографических ключей (например, эти ключи не хранятся на этом же диске).

Рекомендации по криптографической защите информации приведены в разделе 10.

Методы, обеспечивающие безопасную перезапись запоминающего устройства, различаются для запоминающих устройств разного типа. Прежде, чем начать использовать инструментальные средства перезаписи, необходимо убедиться в том, что они применимы к запоминающему устройству данного типа.

11.2.8 Оборудование, оставленное пользователями без присмотра

Средство управления

Обеспечение пользователями соответствующей защиты оборудования, оставленного без присмотра.

Руководство по внедрению

Все пользователи должны быть ознакомлены с требованиями и процедурами безопасности по защите оставленного без присмотра оборудования, а также со своей ответственностью за обеспечение такой защиты. Пользователи должны выполнять следующие рекомендации:

a) прерывать активные сессии после окончания работы, если они не могут быть защищены посредством соответствующего механизма блокирования, например, защищенного паролем «хранителя экрана»;

b) отключаться от приложений и сетевых сервисов после завершения работы с ними;

c) предотвращать несанкционированное использование оставленных без присмотра компьютеров или мобильных устройств посредством блокировки клавиатуры или аналогичного средства управления, например, пароля доступа.

11.2.9 Политика «чистого стола» и «чистого экрана»

Средство управления

Принятие политики «чистого стола» для бумажных документов и съемных запоминающих устройств, а также политики «чистого экрана» для средств обработки информации.

Руководство по внедрению

Политики «чистого стола» и «чистого экрана» должны учитывать классификацию информации (8.2), требования законодательства и договоров (18.1), а также соответствующие риски и организационную культуру. Необходимо принять во внимание следующие рекомендации:

a) чувствительную или критическую бизнес-информацию, например, на бумажных документах или на электронных запоминающих устройствах, когда в ней нет необходимости, особенно перед уходом из офиса, следует запирать (лучше всего в сейфе, шкафу или других надежных предметах мебели);

b) перед тем, как оставить без присмотра компьютеры и терминалы, следует выйти из системы или защитить их с помощью механизма блокировки экрана и клавиатуры, управляемого паролем, токеном или аналогичным механизмом аутентификации пользователя; если компьютеры и терминалы не используются, то они должны быть защищены посредством блокировки клавиатуры, паролей или других средств управления;

c) следует исключить возможность несанкционированного использования фотокопировальных аппаратов и другой копировальной техники (например, сканеров, цифровых камер);

d) носители, содержащие чувствительную или классифицированную информацию, следует немедленно изымать из принтеров.

Дополнительная информация

Политика «чистого стола»/«чистого экрана» снижает риски несанкционированного доступа, утраты или повреждения информации в рабочее и нерабочее время. Сейфы и другие средства безопасного хранения также могут защищать хранящуюся в них информацию в случае чрезвычайных ситуаций, например, пожара, землетрясения, наводнения или взрыва.

Следует рассмотреть возможность применения принтеров с функцией PIN-кодов, обеспечивающей получение распечаток только их создателями и только при нахождении рядом с принтером.

12 Безопасность функционирования

12.1 Операционные процедуры и ответственность

Цель: Обеспечить надлежащее и безопасное функционирование средств обработки информации.

12.1.1 Документирование операционных процедур

Средство управления

Документирование операционных процедур и предоставление их всем пользователям, которым они необходимы.

Руководство по внедрению

Документированные процедуры должны быть подготовлены для операционной деятельности, связанной со средствами обработки и передачей информации, например, процедуры запуска и завершения работы компьютеров, резервного копирования, технического обслуживания оборудования, обращения с носителями данных, а также процедуры обеспечения безопасности помещений с компьютерным и коммуникационным оборудованием.

Операционные процедуры должны регламентироваться инструкциями по эксплуатации, включая:

a) установку и конфигурацию систем;

b) обработку информации и обращение с ней, выполняемых автоматически и вручную;

c) резервное копирование (12.3);

d) требования к планированию заданий, в том числе взаимосвязи с другими системами, время начала выполнения самого раннего задания и время завершения самого последнего задания;

e) инструкции по обработке ошибок или других непредвиденных ситуаций, которые могут возникнуть при выполнении заданий, включая ограничения на использование системных утилит (см. 11.5.4);

f) контакты со службой поддержки и руководством, в том числе контакты с внешней службой поддержки, на случай неожиданных операционных или технических проблем;

g) инструкции по особому обращению с выходными данными и носителями информации, например, по использованию специальных бланков или по управлению конфиденциальными выходными данными, в том числе процедуры безопасной утилизации результатов заданий, завершившихся неудачно (8.3 и 11.2.7);

h) процедуры по перезапуску и восстановлению системы для использования в случае отказа системы;

i) администрирование данных журнала аудита и системного журнала (12.4);

j) процедуры мониторинга.

Операционные процедуры и документированные процедуры для системных операций следует рассматривать как официальные документы, изменения в них вносятся с разрешения руководства. Управлять информационными системами, при наличии технических возможностей, следует единообразно, используя одинаковые процедуры, инструментальные средства и утилиты.

12.1.2 Управление изменениями

Средство управления

Управление изменениями в организации, бизнес-процессах, средствах и системах обработки информации, которые влияют на информационную безопасность.

Руководство по внедрению

В частности, необходимо принять во внимание следующие вопросы:

a) идентификация и регистрация существенных изменений;

b) планирование и тестирование изменений;

c) оценка возможных последствий таких изменений, включая воздействие на безопасность;

d) формальная процедура утверждения предлагаемых изменений;

e) проверка того, все ли требования информационной безопасности были удовлетворены;

f) подробное информирование об изменениях всех заинтересованных лиц;

g) процедуры возврата в исходное состояние, в том числе процедуры и ответственность за аварийное завершение и восстановление в случае неудачного внесения изменений и непредвиденных событий;

h) предоставление процесса аварийных изменений, обеспечивающего быстрое и управляемое внесение необходимых изменений для устранения инцидента (16.1).

С целью обеспечения надлежащего управления всеми изменениями следует формально определить ответственность и разработать соответствующие процедуры управления. При внесении изменений вся необходимая информация должна сохраняться в журнале аудита.

Дополнительная информация

Ненадлежащее управление изменениями в средствах и системах обработки информации является распространенной причиной отказов системы и нарушений безопасности. Изменение среды функционирования, особенно при вводе разработанной системы в эксплуатацию, может повлиять на надежность приложений (см. также 14.2.2).

12.1.3 Управление мощностями

Средство управления

Мониторинг использования ресурсов, их оптимизация в соответствие с потребностями бизнеса, а также прогнозирование будущих потребностей в мощностях, обеспечивающих необходимую производительность системы.

Руководство по внедрению

Потребность в мощностях следует определять с учетом важности для бизнеса соответствующей системы. Для обеспечения и, при необходимости, повышения доступности и эффективности системы следует выполнять ее настройку и мониторинг. Для своевременно выявления проблем следует установить соответствующие средства автоматизации. При прогнозировании будущих потребностей в мощностях следует учитывать новые направления бизнеса и требования к системе, а также текущие и прогнозируемые тенденции относительно возможностей организации по обработке информации

Особое внимание необходимо уделять любым ресурсам с высокой стоимостью, или тем ресурсам, для закупки которых требуется длительное время; следовательно, администраторы, выполняющие управление мощностями, должны проверять использование основных системных ресурсов. Они должны идентифицировать тенденции использования ресурсов, особенно это касается бизнес-приложений или инструментальных средств управления информационными системами.

Администраторы, выполняющие управление мощностями, должны использовать эту информацию для определения и исключения потенциально узких мест, а также зависимости от основного персонала, который может представлять угрозу для безопасности системы или сервисов, планируя соответствующее действие.

Обеспечить достаточные мощности можно посредством их наращивания или снижения потребности в них. Примеры управления потребностью в мощностях включают:

a) удаление устаревших данных (с дискового пространства);

b) вывод из эксплуатации приложений, систем, баз данных или оборудования;

c) оптимизация процессов пакетной обработки и расписаний машинного времени;

d) оптимизация прикладной логики или запросов к базе данных;

e) запрет использования полосы пропускания или ее ограничение для ресурсоёмких сервисов, если они не являются критичными для бизнеса (например, потоковая передача видео).

Для систем, предназначенных для решения критически важных задач, следует разработать и использовать документированный план управления мощностями.

Дополнительная информация

Кроме того, данное средство управления используется применительно к мощности человеческих ресурсов, а также офисов и средств.

12.1.4 Разделение сред разработки, тестирования и эксплуатации

Средство управления

Разделение сред разработки, тестирования и эксплуатации, чтобы снизить риск несанкционированного доступа или внесения изменений в среду эксплуатации.

Руководство по внедрению

Следует определить уровень взаимного разделения сред эксплуатации, тестирования и разработки, необходимый для предотвращения эксплуатационных проблем, и реализовать соответствующие меры.

Необходимо принять во внимание следующие вопросы:

a) следует определить и задокументировать правила перевода статуса программного обеспечения из «разрабатываемого» в «эксплуатируемое»;

b) разрабатываемое и эксплуатируемое программное обеспечение должны работать на разных системах или на разных процессорах компьютера и в различных доменах или каталогах;

c) изменения к действующим операционным системам и приложениям следует предварительно протестировать в среде тестирования или среде отладки до их внесения в действующие системы;

d) во всех случаях, кроме как исключительных, не следует выполнять тестирование на действующих системах;

e) компиляторы, редакторы и другие инструментальные средства разработки или системные утилиты не должно быть доступны из действующих систем, когда это не требуется;

f) пользователи должны использовать разные пользовательские профили для действующей и тестируемой систем, в меню должны отображаться соответствующие идентификационные сообщения, чтобы уменьшить риск ошибки;

g) чувствительные данные не должны копироваться в среду тестирования системы, если в ней не предусмотрены соответствующие средства управления (14.3).

Дополнительная информация

Деятельность, связанная с разработкой и тестированием, может быть причиной серьезных проблем, например, нежелательных изменений файлов или системной среды, а также системных сбоев. В этом случае необходимо поддерживать всем знакомую и стабильную среду тестирования и предотвращать неправомерный доступ разработчиков к среде эксплуатации.

Если занятый разработкой и тестированием персонал имеет доступ к действующей системе и содержащейся в ней информации, то у него

имеется возможность вводить несанкционированные или непроверенные программные коды, либо изменять рабочие данные. В некоторых системах этой возможностью удается злоупотребить для совершения мошенничества либо для ввода непротестированного или вредоносного кода, который может стать причиной серьезных проблем в работе системы.

Занятый разработкой и тестированием персонал может также представлять угрозу для конфиденциальности рабочей информации.

Деятельность, связанная с разработкой и тестированием, может служить причиной непреднамеренных изменений в программном обеспечении или в информации, если вычислительная среда используется совместно. Следовательно, разделение сред разработки, тестирования и эксплуатации целесообразно, оно способствует уменьшению рисков случайного изменения или несанкционированного доступа к рабочему программному обеспечению и бизнес-данным (о защите тестовых данных см. также в 14.3).

12.2 Защита от вредоносных программ

Цель: Обеспечить защиту информации и средств обработки информации от вредоносных программ.

12.2.1 Средства управления защитой от вредоносных программ

Средство управления

Внедрение средств управления защитой от вредоносных программ, обеспечивающих их обнаружение и блокирование, восстановление исходного состояния, а также предназначенных для информирования пользователей.

Руководство по внедрению

Защита от вредоносных программ должна основываться на программном обеспечении, позволяющем обнаруживать эти программы, осведомленности в области информационной безопасности, соответствующих средствах управления доступом к системе и надлежащем управлении изменениями. Необходимо принять во внимание следующие рекомендации:

a) утверждение формальной политики, запрещающей использование несанкционированного программного обеспечения (12.6.2 и 14.2);

b) внедрение средств управления, которые предотвращают или обнаруживают использование несанкционированного программного обеспечения (например, приложение Whitelisting – База доверенных приложений);

c) внедрение средств управления, которые предотвращают или обнаруживают использование известных или подозрительных веб-сайтов с вредоносными программами (например, приложение Blacklisting);

d) утверждение формальной политики для защиты от рисков, связанных с получением файлов и программного обеспечения через внешние сети или с помощью других носителей информации, в которой должно содержаться указание о необходимости принятия защитных мер;

e) уменьшение уязвимостей, которые могут использоваться вредоносными программами, например, посредством управления техническими уязвимостями (смотри 12.6);

f) проведение регулярных инвентаризаций программного обеспечения и содержания данных систем, поддерживающих критические бизнес-процессы. При наличии не утвержденных файлов или несанкционированных поправок следует проводить официальное расследование;

g) установка и регулярное обновление антивирусного программного обеспечения для обнаружения вредоносных программ и восстановления системы, сканирующего компьютеры и носители данных, в качестве профилактической меры или на регулярной основе; выполняемые проверки включают в себя:

1) сканирование перед использованием всех файлов, полученных из сетей или с запоминающих устройств любого типа, на наличие вредоносных программ;

2) сканирование перед использованием любых вложений электронной почты и скачиваемой информации на наличие вредоносных программ; это сканирование следует выполнять в различных местах, например, на серверах электронной почты, персональных компьютерах и на входе сети организации;

3) сканирование веб-страниц на наличие вредоносных программ;

h) определение процедур и ответственности, связанных с защитой от вредоносных программ, проведением тренингов по применению этих процедур, оповещением и восстановлением после атак с применением вредоносных программ;

i) подготовка соответствующих планов обеспечения непрерывности бизнеса для восстановления после атак с применением вредоносных программ, включая все необходимые мероприятия по резервному копированию и восстановлению данных и программного обеспечения (12.3);

j) реализация процедур по регулярному сбору такой информации, как например, подписка на почтовые рассылки и/или проверка веб-сайтов, предоставляющих информацию о новых вредоносных программах;

k) реализация процедур по проверке информации, относящейся к вредоносным программам, а также обеспечение точности и информативности предупреждающих информационных сообщений; для того, чтобы отличать программы-мистификации от реальных вредоносных программ, руководители должны обеспечить возможность использования профессиональных источников, например, респектабельных журналов и заслуживающих доверия Интернет-сайтов, а также программного

обеспечения, обеспечивающего защиту от вредоносных программ, от известных поставщиков; все пользователи должны быть осведомлены о существовании программ-мистификаций и о порядке действий при их обнаружении;

l) изоляция сред, воздействие вредосных программ на которые может закончиться катастрофой.

Дополнительная информация

Повысить эффективность защиты от вредоносных программ может одновременное использование от различных поставщиков двух или более программных продуктов, защищающих среду обработки информации от вредоносных программ.

Следует принять меры для защиты от занесения вредоносных программ во время технического обслуживания и при аварийных ситуациях, когда обычные средства управления защитой от вредоносных программ могут блокироваться.

При определенных условиях защита от вредоносных программ может стать причиной сбоев в работе.

Использование программного обеспечения, обнаруживающего вредоносные программы и восстанавливающего исходное состояние, в качестве единственного средства управления защитой от вредоносных программ в большинстве случаев недостаточно; как правило, оно должно сопровождаться операционными процедурами, которые будут препятствовать занесению вредоносных программ.

12.3 Резервное копирование

Цель: Защитить от потери данных.

12.3.1 Резервное копирование информации

Средство управления

Регулярное создание и тестирование резервных копий информации, программного обеспечения и образов системы в соответствии с установленной политикой резервного копирования.

Руководство по внедрению

Для определения требований организации относительно резервного копирования информации, программного обеспечения и систем следует разработать и утвердить политику резервного копирования.

В политике резервного копирования следует определить требования по сохранности и защите.

Должны быть предусмотрены соответствующие средства резервного копирования, обеспечивающие возможность восстановления всей важной информации и программного обеспечения после чрезвычайной ситуации или повреждения носителей информации.

При разработке плана резервного копирования следует принять во внимание следующие вопросы:

a) создание точных и полных записей со сведениями о резервных копиях и документированных процедур восстановления;

b) объем (например, полное или частичное резервное копирование) и периодичность резервного копирования должны отражать требования бизнес-деятельности организации, требования по безопасности, вовлеченной в процесс информации, а также критичность этой информации для обеспечения непрерывности работы организации;

c) хранение резервных копий в отдаленном месте, на достаточном расстоянии от основной территории, для того, чтобы избежать любого рода их повреждений в случае чрезвычайной ситуации;

d) обеспечение для резервных копий информации надлежащего уровня защиты от физических угроз и факторов окружающей среды (раздел 11) согласно стандартам, действующим на основной территории;

e) выполнение регулярного тестирования носителей с резервными копиями для обеспечения уверенности в том, что в случае возникновения чрезвычайных ситуаций нужные данные будут доступны и ими можно будет воспользоваться; процедуры тестирования носителей следует выполнять вместе с процедурами восстановления, чтобы оценить время, необходимое для восстановления. Тестирование возможности восстановления зарезервированных данных должно выполняться на предназначенном для тестирования носителе, без переписывания данных на оригинальном (исходном) носителе в том случае, когда процесс резервного копирования или восстановления завершится неудачно и это станет причиной непоправимого повреждения или потери данных;

f) защита резервных копий посредством шифрования в тех случаях, когда имеет значение конфиденциальность информации.

Посредством операционных процедур следует контролировать выполнение резервного копирования и устранять сбои запланированного резервного копирования, это позволит обеспечить комплектность резервных копий в соответствии с политикой резервного копирования.

Следует регулярно проверять планы резервного копирования для отдельных систем и сервисов на предмет их соответствия требованиям планов обеспечения непрерывности бизнеса. Для критичных систем и сервисов планы резервного копирования должны охватывать всю системную информацию, приложения и данные, необходимые для полного восстановления системы в случае чрезвычайной ситуации.

Следует определить срок хранения основной бизнес-информации с учетом всех требований к архивным копиям постоянного хранения.

12.4 Регистрация и мониторинг

Цель: Фиксировать события и предоставлять свидетельства.

12.4.1 Регистрация событий

Средство управления

Создание, хранение и регулярный просмотр журналов, предназначенных для регистрации действий пользователей, исключительных ситуаций, сбоев и событий, связанных с информационной безопасностью.

Руководство по внедрению

Журналы регистрации должны содержать следующие данные, если последние являются существенными:

a) идентификаторы пользователей;

b) фунционирование системы;

c) дату, время и подробности важных событий, например, входа в систему и выхода из нее;

d) идентификацию устройства и его местонахождение, если возможно, и системный идентификатор;

e) записи успешных и отклоненных попыток доступа к системе;

f) записи успешных и отклоненных попыток доступа к данным и другим активам;

g) изменения в конфигурации системы;

h) использование привилегий;

i) использование системных утилит и приложений;

j) доступ к файлам и вид доступа;

k) сетевые адреса и протоколы;

l) сигналы тревоги, поданные системой управления доступом;

m) активация и деактивация систем защиты, например, системы антивирусной защиты и системы обнаружения вторжений;

n) записи транзакций, выполненных пользователями в приложениях.

На совокупности регистрируемых событий основана автоматизированная система мониторинга, которая способна генерировать сводную информацию о сообщениях и предупреждениях системы безопасности.

Дополнительная информация

Журналы регистрации могут содержать чувствительные данные и персональную информацию, позволяющую установить личность. Следует предпринять надлежащие меры по защите приватности (18.1.4).

При наличии возможности, системным администраторам следует запретить уничтожать или деактивировать журналы, в которых регистрируются их собственные действия (12.4.3).

12.4.2 Защита информации журналов регистрации

Средство управления

Защита средств регистрации событий и информации журналов регистрации от несанкционированного вмешательства и несанкционированного доступа.

Руководство по внедрению

Средства управления должны обеспечивать защиту средств регистрации от несанкционированных изменений и эксплуатационных проблем, к которым относятся:

a) изменения в типах регистрируемых сообщений;

b) редактирование или удаление файлов системных журналов;

c) исчерпание объема памяти, выделенной под системный журнал на носителе информации, что приводит либо к невозможности регистрации событий, либо к перезаписи последних зарегистрированных событий поверх уже записанных.

Для некоторых журналов аудита может потребоваться архивация в качестве составной части политики хранения записей или в связи с требованиями к сбору и хранению свидетельств (16.1.7).

Дополнительная информация

Системные журналы часто содержат большой объем информации, значительная часть которой является излишней для мониторинга информационной безопасности. Чтобы облегчить идентификацию событий, которые являются существенными для целей мониторинга безопасности, следует рассмотреть возможность автоматического копирования сообщений соответствующего типа во второй журнал или применения подходящих системных утилит и инструментальных средств аудита для выполнения анализа и рационализации файла.

Системные журналы нуждаются в защите, поскольку, при наличии возможности изменять или удалять содержащиеся в них данные, может создаться ложное представление о безопасности. Защитить журналы можно посредством их копирования в режиме реального времени извне системы, управляемой системным администратором или оператором.

12.4.3 Журналы регистрации действий администратора и оператора

Средство управления

Регистрация действий системного администратора и системного оператора, а также защита и регулярная проверка журналов регистрации их действий.

Руководство по внедрению

Держатели учетной записи привилегированного пользователя могут иметь возможность манипулировать журналами посредством средств обработки информации, находящихся под их непосредственным управлением; следовательно, для обеспечения подотчетности

привилегированных пользователей необходимо защищать и проверять журналы регистрации их действий.

Дополнительная информация

Для мониторинга соответствия принятым нормам деятельности по системному и сетевому администрированию можно использовать систему обнаружения вторжений, управляемую извне зоны, контролируемой системными и сетевыми администраторами.

12.4.4 Синхронизация часов

Средство управления

Синхронизация часов всех важных систем обработки информации внутри организации или домена безопасности с соответствующим источником сигналов точного времени.

Руководство по внедрению

Следует задокументировать внешние и внутренние требования по представлению времени, синхронизации и обеспечению точности хода часов. Могут использоваться требования законодательства, нормативно-правовых актов, соответствующих стандартов или внутреннего мониторинга. Следует определить стандартное время, используемое в организации.

Следует задокументировать и внедрить в организации надежный метод получения сигналов от внешнего источника (источников) точного времени для синхронизации ее внутренних часов.

Дополнительная информация

Правильная установка внутренних часов компьютера имеет важное значение для обеспечения точности журналов аудита, которые могут потребоваться для расследований или в качестве свидетельства при рассмотрении судебных дел или дисциплинарных проступков. Неточные журналы аудита могут помешать подобным расследованиям и повредить достоверности таких свидетельств. В качестве эталонных часов для систем регистрации можно использовать часы, которые связаны с радиовещательной службой точного времени, использующей показания атомных часов. Для обеспечения синхронизации всех серверов с эталонными часами можно использовать сетевой протокол синхронизации времени.

12.5 Управление эксплуатируемым программным обеспечением

Цель: Обеспечить целостность эксплуатируемых систем.

12.5.1 Установка программного обеспечения в эксплуатируемые системы

Средство управления

Внедрение процедур управления установкой программного обеспечения в эксплуатируемые системы.

Руководство по внедрению

Для управления заменой программного обеспечения в эксплуатируемых системах следует принять во внимание следующие рекомендации:

a) обновление системного программного обеспечения, приложений и библиотек программ должно осуществляться только подготовленными администраторами после соответствующего разрешения руководства (9.4.5);

b) эксплуатируемые системы должны содержать только проверенный исполняемый код, но не код, находящийся в процессе разработки, и не средства компиляции;

c) приложения и системное программное обеспечение должны внедряться только после исчерпывающего и успешного тестирования; тестирование должно включать выполнение тестов на практичность, безопасность, влияние на другие системы и на удобство использования, они должны выполняться на отдельных системах (12.1.4); необходимо обеспечить обновление всех соответствующих библиотек исходного кода программ;

d) следует использовать систему управления конфигурациями для поддержания управления всем внедренным программным обеспечением, а также системной документацией;

e) перед реализацией изменений необходимо разработать стратегию отката (восстановления исходного состояния);

f) необходимо в журнале аудита регистрировать все обновления библиотек системного программного обеспечения;

g) следует сохранять предыдущие версии прикладного программного обеспечения на случай их применения в качестве чрезвычайной меры;

h) старые версии программного обеспечения надлежит хранить в архиве вместе со всей необходимой информацией и параметрами, процедурами, описанием конфигурации и вспомогательным программным обеспечением до тех пор, пока в архиве хранятся соответствующие данные.

Программное обеспечение, приобретенное у поставщиков и применяемое в эксплуатируемых системах, должно поддерживаться на уровне, который предусматривают поставщики программного обеспечения. Через некоторое время поставщики программного обеспечения прекращают поддерживать старые версии программного обеспечения. Организация должна принимать во внимание риски, связанные с

использованием программного обеспечения, техническая поддержка которого не производится.

Любое решение по переходу на новую версию должно приниматься с учетом требований бизнеса к изменениям, а также безопасности этой версии, то есть с учетом появления новых функциональных возможностей информационной безопасности или количества и серьезности вопросов информационной безопасности, связанных с этой версией. Программные «заплатки» (патчи) следует применять в том случае, если они могут помочь устранить или уменьшить уязвимости информационной безопасности (12.6).

Физический и логический доступ должен предоставляться представителям поставщика только в целях технической поддержки и с разрешения руководства. Деятельность представителей поставщика должна осуществляться под надзором (15.2.1).

Компьютерное программное обеспечение может использовать программы и модули от сторонних поставщиков, для этих программ и модулей следует предусмотреть мониторинг и управление, чтобы избежать несанкционированных изменений, способных внести уязвимости в безопасность организации.

12.6 Управление техническими уязвимостями

Цель: Предотвратить использование технических уязвимостей.

12.6.1 Управление техническими уязвимостями

Средство управления

Своевременное получение информации о технических уязвимостях информационных систем, оценка подверженности организации подобным уязвимостям и принятие надлежащих мер для реагирования на связанный с этими уязвимостями риск.

Руководство по внедрению

Текущий и полный перечень активов (раздел 8) - предпосылка эффективного управления техническими уязвимостями. Для управления техническими уязвимостями необходима конкретная информация, включающая в себя сведения о поставщике программного обеспечения, номерах версий, текущем состоянии развертывания (например, какое программное обеспечение и на каких системах установлено), а также о лице (лицах) в организации, ответственном(ых) за программное обеспечение.

При обнаружении потенциальных технических уязвимостей следует своевременно предпринять соответствующие меры. Для организации эффективного процесса управления техническими уязвимостями необходимо следовать нижеприведенным рекомендациям:

a) в организации следует определить, а также назначить роли и ответственность, связанные с управлением техническими уязвимостями, включая мониторинг уязвимостей, определение рисков уязвимостей, внесение «заплаток», отслеживание активов и необходимую ответственность в части координации этих работ;

b) для программного обеспечения и другого технического оборудования следует определить информационные активы, которые будут использоваться для выявления соответствующих технических уязвимостей и обеспечения осведомленности о них (на основе инвентаризационной описи, см. 8.1.1); эти информационные активы следует обновлять по результатам инвентаризации, либо при нахождении других новых или полезных активов;

c) следует определить сроки реагирования на уведомления о технических уязвимостях, потенциально актуальных для организации;

d) после обнаружения потенциальной технической уязвимости организация должна определить связанные с ней риски и меры, которые следует предпринять; данные меры могут включать внесение «заплаток» в уязвимые системы и/или применение других средств управления;

e) в зависимости от того, насколько срочно необходимо устранить проблему, связанную с технической уязвимостью, предпринимаемые меры должны осуществляться в соответствии с процедурами управления внесением изменений (12.1.2) или в соответствии с процедурами реагирования на инциденты информационной безопасности (13.2);

f) при наличии возможности получить «заплатку» из доверенного источника следует оценить риски, связанные с внесением «заплатки» (риск, создаваемый уязвимостью, следует сравнить с риском, возникающим в результате внесением «заплатки»);

g) «заплатки» перед установкой следует протестировать и оценить, это позволит обеспечить их эффективность и отсутствие неприемлемых побочных эффектов; в случае отсутствия «заплаток» следует рассмотреть другие средства управления, например:

1) отключение сервисов или возможностей, связанных с уязвимостью;

2) приспособление (адаптация) или добавление средств управления доступом, например, межсетевых экранов на границах сетей (13.1);

3) усиленный мониторинг для обнаружения или предотвращения реальных атак;

4) повышение осведомленности об уязвимости;

h) для всех предпринимаемых процедур необходимо вести журнал аудита;

i) следует регулярно проводить мониторинг и оценку процесса управления техническими уязвимостями, чтобы обеспечить его эффективность и результативность;

j) системам с высоким уровнем риска следует уделять первоочередное внимание;

k) для обеспечения передачи данных об уязвимостях к функции реагирования на инциденты и для обеспечения технических процедур, которые нужно будет выполнить, когда произойдет инцидент, следует эффективный процесс управления техническими уязвимостями объединить с деятельностью по управлению инцидентами;

l) следует определить процедуру управления ситуацией, когда уязвимость была выявлена, но соответствующая контрмера отсутствует. В этой ситуации организация должна оценить риск, связанный с известной уязвимостью, и определить соответствующие превентивные и корректирующие меры.

Дополнительная информация

Управление техническими уязвимостями можно рассматривать как подфункцию управления изменениями; вследствие этого допускается применение процессов и процедур управления изменениями при управлении техническими уязвимостями (12.1.2, 14.2.2).

Поставщики программного обеспечения часто находятся под давлением необходимости как можно скорее выпускать программные «заплатки», поэтому в некоторых случаях внесение программной «заплатки» не сможет решить проблему адекватным образом, а станет причиной отрицательных побочных эффектов. Кроме того, в некоторых случаях после внесения программной «заплатки», выполнить ее удаление будет затруднительно.

Если адекватное тестирование программных «закладок» невозможно, например, по причине высокой стоимости или недостатка ресурсов, то следует рассмотреть вопрос о том, чтобы отложить внесение программной «закладки» до оценки связанных с ней рисков на основе опыта других пользователей. Возможно, будет полезно использовать стандарт O‘z DSt ISO/IEC 27031.

12.6.2 Ограничения на установку программного обеспечения

Средство управления

Разработка и внедрение правил установки программного обеспечения пользователями.

Руководство по внедрению

Организация должна определить и соблюдать строгую политику относительно того, кто из пользователей может устанавливать программное обеспечение.

При разработке этой политики должен применяться принцип наименьших (минимальных) привилегий. Если пользователям предоставлены определенные привилегии, они могут иметь возможность устанавливать программное обеспечение. Организация должна определить, установка каких видов программного обеспечения разрешена (например,

новых версий программного обеспечения и «заплаток» для системы безопасности в существующем программном обеспечении), а установка каких видов программного обеспечения запрещена (например, программного обеспечения, предназначенного только для персонального использования, и потенциально вредоносного программного обеспечения, источник происхождения которого неизвестен или вызывает подозрение).

Эти привилегии следует предоставлять тем пользователям, которым присвоены соответствующие роли.

Дополнительная информация

Неконтролируемая установка программного обеспечения на вычислительных устройствах может стать причиной появления уязвимостей и, как следствие этого, причиной утечки и нарушения целостности информации или других инцидентов информационной безопасности, или нарушения прав интеллектуальной собственности.

12.7 Аудит информационных систем

Цель: Минимизировать влияние аудиторской деятельности на эксплуатируемые системы.

12.7.1 Средства управления аудитом информационных систем

Средство управления

Тщательное планирование и согласование требований к аудиту и аудиторской деятельности, связанных с выполнением проверок на эксплуатируемых системах для сведения к минимуму риска нарушения бизнес-процессов.

Руководство по внедрению

Необходимо соблюдать следующие рекомендации:

a) требования к аудиту следует согласовать с соответствующим руководством;

b) объем тестирования при проведении технического аудита следует согласовать и контролировать;

c) аудиторское тестирование должно ограничиваться доступом к программному обеспечению и данным только для чтения;

d) доступ, предполагающий не только чтение, следует разрешать только для изолированных копий системных файлов, которые должны быть удалены по завершению аудита; либо для этих файлов должна быть обеспечена соответствующая защита, если существует обязанность сохранять подобные файлы в соответствии с требованиями к документации аудита;

e) следует определить и согласовать требования к специальной или дополнительной обработке;

f) аудиторское тестирование, которое может повлиять на доступность системы, следует выполнять во внерабочее время;

g) следует обеспечить мониторинг всех сеансов доступа и их регистрацию в специально созданном журнале.

13 Безопасность обмена информацией

13.1 Управление сетевой безопасностью

Цель: Обеспечить защиту информации в сетях и поддерживающих ее средств обработки информации.

13.1.1 Средства управления сетью

Средство управления

Обеспечение управления и контроля сетями с целью защиты информации в системах и приложениях.

Руководство по внедрению

Следует внедрить средства управления, обеспечивающие безопасность информации в сетях и защиту связанных с ними сервисов от несанкционированного доступа. В частности, необходимо рассмотреть следующие вопросы:

a) следует установить ответственность и процедуры по управлению сетевым оборудованием;

b) при необходимости ответственность за функционирование сети и компьютеров следует разделить (6.1.2);

c) следует внедрить специальные средства управления для обеспечения конфиденциальности и целостности данных, передаваемых по сетям общего пользования, а также для защиты подключенных систем (раздел 10 и 13.2). Для поддержания доступности сетевых серверов и подключенных компьютеров могут также потребоваться специальные средства управления;

d) необходимо использовать регистрацию событий и мониторинг, а также обнаружение действий, которые могут повлиять на информационную безопасность или имеют отношение к обеспечению;

e) действия по управлению следует тщательно координировать, это позволит оптимизировать предоставляемые для организации сервисы и обеспечить согласованное применение средств управления во всей инфраструктуре обработки информации;

f) системы в сети следует аутентифицировать;

g) соединение систем с сетью следует ограничивать.

Дополнительная информация

Более подробная информация по сетевой безопасности приведена в O‘z DSt ISO/IEC 27033-1, O‘z DSt ISO/IEC 27033-2, O‘z DSt ISO/IEC 27033-3, O‘z DSt ISO/IEC 27033-4, O‘z DSt ISO/IEC 27033-5.

13.1.2 Безопасность сетевых сервисов

Средство управления

Определение и включение во все соглашения о предоставлении сетевых сервисов механизмов безопасности, уровней обслуживания и требований по управлению всеми сетевыми сервисами, независимо от того, предоставляются ли данные сервисы самой организацией или специализированной сторонней организацией.

Руководство по внедрению

Необходимо определить и периодически подвергать мониторингу способность провайдера сетевых сервисов безопасно управлять оговоренными сервисами, также следует оговорить право на проведение аудита.

Следует определить меры обеспечения безопасности, необходимые для определенных сервисов, например, характеристики безопасности, уровни обслуживания и требования по управлению. Организации следует предоставить возможность внедрения данных мер провайдером сетевых сервисов.

Дополнительная информация

Сетевые сервисы включают в себя предоставление соединений, сервисы частных сетей, а также сети с дополнительными возможностями и решения, обеспечивающие безопасность управляемых сетей, например, межсетевые экраны и системы обнаружения вторжений. Для данных сервисов могут быть использованы как простые фильтры с неуправляемыми полосами пропускания, так и сложные решения с дополнительными услугами.

Характеристиками безопасности сетевых сервисов являются:

a) технологии, применяемые для безопасности сетевых сервисов, например, аутентификация, шифрование и средства управления сетевыми соединениями;

b) технические параметры, требуемые для безопасного соединения с сетевыми сервисами в соответствии с правилами обеспечения безопасности и установления сетевых соединений;

c) процедуры для использования в сетевых сервисах для ограничения доступа, где это необходимо, к сетевым сервисам и приложениям.

13.1.3 Разделение в сетях

Средство управления

Разделение в сетях различных групп информационных сервисов и систем, а также пользователей.

Руководство по внедрению

Одним из методов управления безопасностью больших сетей является их разделение на отдельные сетевые домены.

Выбор доменов может основываться на уровнях доверия (например, общедоступный домен, домен рабочего стола, домен сервера), на подразделениях организации (например, отдел кадров, бухгалтерия, отдел маркетинга) или на некоторой их комбинации (например, домен сервера, соединяющийся со многими подразделениям организации). Разделение может быть выполнено посредством использования физически или логически разделенных сетей (например, виртуальных частных сетей).

Периметр каждого домена следует хорошо определить. Доступ между сетевыми доменами допускается, но он должен быть управляемым в периметре, использовавшем шлюз (например, межсетевой экран, фильтрующий маршрутизатор). Критерии разделения сетей на домены и разрешение доступа через шлюзы должны быть основаны на определенных требованиях по безопасности для каждого домена. Определение этих требований по безопасности следует выполнять с учетом политики управления доступом (9.1.1), требований к доступу, ценности и классификации обрабатываемой информации, а также с учетом относительной стоимости и влияния на производительность внедрения соответствующей технологии межсетевого интерфейса.

Беспроводные сети требуют специальной обработки из-за нечетко определенного сетевого периметра. Для чувствительных сред беспроводный доступ следует рассматривать как внешние соединения, также следует рассмотреть вопрос об отделении беспроводных сетей от внутренних сетей посредством шлюза и предоставления беспроводного доступа к внутренним системам в соответствии с политикой средств управления сетью (13.1.1).

Непосредственные беспроводные соединения с внутренней сетью организации можно обеспечивать посредством правильной реализации аутентификации, шифрования, современных технологий управления сетевым доступом на пользовательском уровне и стандартов беспроводных сетей.

Дополнительная информация

По мере формирования партнерских отношений, для которых может потребоваться объединение или совместное использование средств обработки информации и сетевых ресурсов, сети все чаще выходят за традиционные рамки организации. Такие расширения могут увеличить риск несанкционированного доступа к информационным системам организации, которая использует сеть; некоторым из этих систем из-за их чувствительности или критичности потребуется защита от других пользователей сети.

13.2 Передача информации

Цель: Поддерживать безопасность информации, передаваемой как внутри организации, так и за ее пределы любым сторонним организациям.

13.2.1 Политики и процедуры передачи информации

Средство управления

Разработка соответствующей формальной политики, а также процедур и средств управления для защиты передачи информации с помощью всех видов средств телекоммуникаций.

Руководство по внедрению

К процедурам и средствам управления, которые надлежит соблюдать при использовании средств телекоммуникаций для передачи информации, относятся:

a) разработанные процедуры защиты передаваемой информации от перехвата, копирования, модификации, неправильной маршрутизации и уничтожения;

b) процедуры обнаружения и защиты от вредоносных программ, которые могут передаваться посредством использования телекоммуникаций (12.2.1);

c) процедуры защиты передаваемой чувствительной электронной информации, присоединяемой к сообщению электронной почты;

d) политика или рекомендации, определяющие допустимое использование средств телекоммуникаций (8.1.3);

e) персонал организации, сотрудники сторонней организации и другие пользователи являются ответственными за недопущение компрометации организации, например, путём распространения клеветы, домогательств и преднамеренного причинения беспокойства, выдачи себя за другое лицо, пересылки цепных писем, несанкционированных покупок и т. п.;

f) использование криптографических методов, например, для защиты конфиденциальности, целостности и подлинности информации (раздел 10);

g) рекомендации по хранению и утилизации всей деловой корреспонденции, включая сообщения, в соответствии с действующим законодательством и нормативно-правовыми актами;

h) средства управления и ограничения, связанные с использованием средств телекоммуникаций, например, автоматическая рассылка сообщений электронной почты по внешним адресам;

i) напоминание персоналу о необходимости принимать надлежащие меры предосторожности во избежание разглашения конфиденциальной информации;

j) напоминание персоналу о том, что недопустимо оставлять без присмотра автоответчики, поскольку сообщения, содержащие конфиденциальную информацию, могут быть прослушаны неуполномоченными лицами, сохранены в системах общего пользования или сохранены ошибочно в результате неправильного набора номера;

k) напоминание персоналу о возможных рисках, присущих использованию факсимильных аппаратов или сервисов, а именно:

1) несанкционированный доступ к встроенной памяти для поиска сообщений;

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

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

Кроме того, персоналу следует напоминать о том, что не следует вести конфиденциальные разговоры в общественных местах или по незащищенным каналам телекоммуникаций, в открытых офисах и в помещениях для переговоров без звукоизоляции.

Сервисы передачи информации должны удовлетворять соответствующим требованиям законодательства (18.1).

Дополнительная информация

Передача информации может происходить с помощью ряда средств телекоммуникаций различного вида, включая электронную почту, голосовую связь, факсимильную и видеосвязь.

Передача программного обеспечения может происходить с помощью различных носителей, включая загрузку из сети Интернет и приобретение у поставщиков, продающих готовые программные продукты.

Следует рассмотреть последствия с точки зрения бизнеса, законодательства и обеспечения безопасности, связанные с электронным обменом данных, электронной торговлей и телекоммуникациями, а также требования к средствам управления.

13.2.2 Соглашения о передаче информации

Средство управления

Заключение соглашений о безопасной передаче бизнес-информации между организацией и сторонними организациями.

Руководство по внедрению

Соглашения о передаче информации должны включать следующее:

a) ответственность руководства за управление передачей и уведомлениями об отправке и получении информации;

b) процедуры обеспечения отслеживаемости и неотказуемости;

c) минимальные технические требования к созданию и передаче пакетов данных;

d) соглашения по условному депонированию;

e) требования по идентификации курьеров;

f) обязательства и ответственность в случае инцидентов информационной безопасности, например, при потере данных;

g) использование согласованной системы маркировки чувствительной или критически важной информации, обеспечивающей немедленное определение значения этой маркировки и соответствующую защиту информации;

h) технические требования к записи и считыванию информации, а также программного обеспечения;

i) любые специальные средства управления, которые необходимы для защиты чувствительных данных, например, средства криптографической защиты информации (10.1);

j) непрерывная поддержка обеспечения безопасности информации в процессе ее передачи;

k) приемлемые уровни управления доступом.

Следует установить и поддерживать политики, процедуры и стандарты по защите информации и транспортировке физических носителей (8.3.3), на них следует ссылаться в вышеупомянутых соглашениях о передаче.

Содержание любого из соглашений, относящееся к вопросам безопасности, должно отражать уровень чувствительности передаваемой бизнес-информации.

Дополнительная информация

Соглашения можно заключать в электронном виде или подписывать вручную, они могут иметь форму официальных контрактов. Использование специальных механизмов при передаче конфиденциальной информации следует согласовывать со всеми организациями во всех видах соглашений.

13.2.3 Электронный обмен сообщениями

Средство управления

Соответствующая защита информации, содержащейся в электронных сообщениях.

Руководство по внедрению

При обеспечении информационной безопасности электронного обмена следует принять во внимание следующие вопросы:

a) защита сообщений от несанкционированного доступа, модификации или отказа в обслуживании в соответствии с системой классификации информации, принятой в организации;

b) обеспечение правильной адресации и доставки сообщения;

c) надежность и доступность сервиса;

d) требования законодательства, например, требования к электронным цифровым подписям;

e) получение санкции на использование внешних общедоступных сервисов, например, мгновенного обмена сообщениями, социальных сетей или совместного использования файлов;

f) более строгие уровни аутентификации при управлении доступом из общедоступных сетей.

Дополнительная информация

Существует множество видов электронного обмена сообщениями, например, электронная почта, электронный обмен данными и социальные сети, которые играют важную роль в обмене бизнес-информацией.

13.2.4 Соглашения о соблюдении конфиденциальности или неразглашении информации

Средство управления

Определение, периодический пересмотр и документирование требований, отражающих потребность организации в защите информации, для соглашений о соблюдении конфиденциальности или неразглашении информации.

Руководство по внедрению

Требования по защите конфиденциальной информации в соглашениях о соблюдении конфиденциальности или неразглашении информации следует формулировать, используя законодательно установленную терминологию. Соглашения о соблюдении конфиденциальности или неразглашении информации заключаются со сторонними организациями или персоналом организации. Элементы данного соглашения следует выбирать или добавлять с учетом типа сторонней организации, а также разрешений на доступ к информации и ее обработку. При идентификации требований в соглашениях о соблюдении конфиденциальности или неразглашении информации следует учесть следующие элементы:

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

b) предполагаемый срок действия соглашения, включая случаи, когда может быть потребуется обеспечивать конфиденциальность в течение неопределенного времени;

c) необходимые действия в случае расторжения соглашения;

d) ответственность и действия подписантов для предотвращения несанкционированного раскрытия информации;

e) каким образом право собственности на информацию, производственные секреты и интеллектуальная собственность связаны с защитой конфиденциальной информации;

f) разрешение на использование конфиденциальной информации и права подписанта на использование информации;

g) право осуществления аудита и мониторинга деятельности, связанной с использованием конфиденциальной информации;

h) процесс уведомления и отчетности о несанкционированном раскрытии или утечке конфиденциальной информации;

i) порядок возврата или уничтожения информации при прекращении действия соглашения;

j) предполагаемые действия, выполнение которых потребуется в случае нарушения условий соглашения.

Кроме того, в соглашение о соблюдении конфиденциальности или неразглашении информации возможно потребуется включение дополнительных элементов, основанных на требованиях информационной безопасности организации.

Соглашения о соблюдении конфиденциальности или неразглашении должны соответствовать всем применимым законодательным и нормативно-правовым актам органов, под юрисдикцию которых попадают соответствующие организации (18.1).

Соглашения о соблюдении конфиденциальности или неразглашении должны пересматриваться периодически и при изменении обстоятельств, которые влияют на их требования.

Дополнительная информация

Соглашения о соблюдении конфиденциальности или неразглашении защищают информацию организации и информируют подписантов об их ответственности за защиту, использование и раскрытие информации надежным и санкционированным способом.

Возможно, что при других обстоятельствах организации потребуется использование других форм соглашения о соблюдении конфиденциальности или неразглашении.

14 Приобретение, разработка и обслуживание информационных систем

14.1 Требования по безопасности информационных систем

Цель: Обеспечить, чтобы информационная безопасность стала неотъемлемой частью информационных систем в течение всего их жизненного цикла, а также установить требования к информационным системам, которые предоставляют сервисы по общедоступным сетям.

14.1.1 Анализ и спецификация требований информационной безопасности

Средство управления

Включение требований информационной безопасности в требования к новым или модернизируемым существующим информационным системам.

Руководство по внедрению

Требования информационной безопасности следует определять посредством использования различных методов, например, путем заимствования соответствующих требований из политик и нормативно-правовых актов, моделей угроз, анализа инцидентов или использования пороговых (предельных) значений уязвимости. Полученные в результате определения требования следует задокументировать и согласовать со всеми заинтересованными сторонами.

Требования информационной безопасности и средства управления должны учитывать важность используемой информации для бизнеса (8.2), а также потенциальный ущерб бизнесу, который может быть нанесен ему в случае отсутствия надлежащего обеспечения безопасности.

Определение требований информационной безопасности и управление связанными с ними процессами должны быть интегрированы в проекты информационных систем на самых ранних стадиях. В результате предварительного обсуждения требований информационной безопасности, например, на стадии проектирования, могут быть найдены более эффективные технико-экономические решения.

Требования информационной безопасности также должны учитывать:

a) необходимый уровень достоверности предъявляемой идентификационной информации пользователями, обуславливающий требования к аутентификации пользователя;

b) процессы предоставления доступа и авторизации для бизнес-пользователей, а также для привилегированных пользователей или сотрудников служб технической поддержки;

c) информированность пользователей и операторов об их обязанностях и ответственности;

d) необходимость защиты активов, особенно относительно обеспечения их доступности, конфиденциальности и целостности;

e) требования, вытекающие из бизнес-процессов, например, требования к регистрации и мониторингу транзакций, требования к неотказуемости;

f) требования, предписанные другими средствами управления безопасностью, например, интерфейсами регистрации и мониторинга или системами обнаружения утечки данных.

Для приложений, посредством которых предоставляются сервисы по общедоступным сетям или которые реализуют транзакции, следует предусмотреть специальные средства управления в 14.1.2 и 14.1.3.

Если программные продукты закупаются, то необходимо следовать официальной процедуре тестирования и закупки. В контрактах с поставщиком должны учитываться установленные требования по безопасности. Если функциональные возможности безопасности в предложенном программном продукте не удовлетворяют установленным

требованиям, то перед закупкой программного продукта необходимо оценить возникающие при этом риски и повторно рассмотреть связанные с этими рисками средства управления.

Следует оценить и внедрить представленное руководство по конфигурации безопасности продукта, соответствующее окончательной версии программного обеспечения/пакета сервисов системы.

Следует определить критерии приемки продуктов, например, относительно их функциональных возможностей, которые придадут уверенность в том, что определенные требования безопасности удовлетворены. Продукты перед закупкой следует оценить по этим критериям. Следует выполнить анализ дополнительных функциональных возможностей, чтобы убедиться в том, что они не внесут дополнительных неприемлемых рисков.

Дополнительная информация

Для определения средств управления, удовлетворяющих требованиям информационной безопасности, следует воспользоваться рекомендациями по управлению рисками, представленными в O‘z DSt ISO/IEC 27005.

14.1.2 Безопасность сервисов приложений в общедоступных сетях

Средство управления

Защита информации сервисов приложений, передаваемой по общедоступным сетям, от мошеннической деятельности, споров по контрактам, а также от несанкционированного раскрытия и модификации.

Руководство по внедрению

При обеспечении информационной безопасности сервисов приложений, передаваемых по общедоступным сетям, следует принимать во внимание следующие факторы:

a) уровень достоверности предъявляемой идентификационной информации, например, в ходе аутентификации, который каждая из сторон требует от другой стороны;

b) процессы авторизации, связанные с теми, кто имеет право утверждать содержимое, выпускать или подписывать основные транзакционные документы;

c) обеспечение полной осведомленности взаимодействующих партнеров о своих авторизациях для предоставления или использования сервиса;

d) определение и удовлетворение требований конфиденциальности, целостности, доказательств отправки и получения основных документов, а также обеспечение неотказуемости от обязательств, например, тендеров и контрактов;

e) требуемый уровень доверия к целостности основных документов;

f) требования по защите любой конфиденциальной информации;

g) конфиденциальность и целостность любых транзакций, связанных с заказом, а также сведений об оплате, точного адреса для доставки и подтверждения о получении;

h) уровень проверки, предпринимаемой для подтверждения сведений об оплате, представленных заказчиком;

i) выбор наиболее приемлемой формы оплаты для защиты от мошенничества;

j) уровень защиты, необходимый для поддержания конфиденциальности и целостности информации заказа;

k) предотвращение потерь и дублирования информации транзакции;

l) ответственность, связанная с любыми мошенническими транзакциями;

m) требования к страхованию.

Многие из вышеупомянутых вопросов могут быть решены посредством средств криптографической защиты информации (раздел 10), с учетом соответствия законодательным требованиям (раздел 18, в частности 18.1.5 по законодательству в области криптографии).

Соглашения о сервисе приложений между партнерами должны быть подкреплены документированным соглашением, в котором зафиксированы условия предоставления сервисов, в том числе подробные сведения об авторизации (см. перечисление b) выше).

Следует учитывать требования к отказоустойчивости при осуществлении атак, которые могут включать требования по защите задействованных серверов приложений или требования по обеспечению доступности межсетевого взаимодействия, необходимого для предоставления сервиса.

Дополнительная информация

Приложения, доступные по общедоступным сетям, подвержены различным сетевым угрозам, например, таким как мошенническая деятельность, споры по контрактам или раскрытие информации. Следовательно, необходимо выполнять подробное определение рисков и выбирать соответствующие средства управления. Необходимые средства управления часто включают криптографические методы для аутентификации и обеспечения безопасной передачи данных.

Для уменьшения рисков для сервисов приложений могут использоваться безопасные методы аутентификации, например, криптография с открытым ключом и электронные цифровые подписи (раздел 10). Там, где необходимы такие сервисы, можно использовать доверенные третьи стороны.

14.1.3 Защита транзакций сервисов приложений

Средство управления

Защита информации, задействованной в транзакциях сервисов приложений, для предотвращения незавершенной передачи данных,

ошибочной маршрутизации, несанкционированного изменения сообщений, несанкционированного раскрытия информации, несанкционированного дублирования или повторной передачи.

Руководство по внедрению

При обеспечении информационной безопасности транзакций сервиса приложений следует принимать во внимание следующие факторы:

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

b) все аспекты транзакции, то есть необходимо обеспечить, что:

1) секретная информация аутентификации пользователей обеих сторон достоверна и проверена;

2) сохраняется конфиденциальность транзакции;

3) сохраняется приватность, связанная со всеми участвующими сторонами;

c) использование зашифрованного канала телекоммуникаций между всеми участвующими сторонами;

d) использование защищенных протоколов для обмена информацией между всеми участвующими сторонами;

e) место хранения сведений о транзакциях должно находиться вне общедоступной среды, например, на аппаратной платформе для хранения данных, находящейся во внутренней сети организации; информация не должна сохраняться и находиться на носителе данных, непосредственно доступном из сети Интернет;

f) при использовании доверенного удостоверяющего центра (например, для издания и поддержки электронных цифровых подписей и/или цифровых удостоверений), безопасность является комплексной и применяется на всем протяжении цикла процесса управления этими подписями/удостоверениями.

Дополнительная информация

Объем применяемых средств управления необходимо соразмерять с уровнем риска, связанным с каждым видом транзакции сервиса приложений.

Может потребоваться согласование транзакций с законами, правилами и нормами той юрисдикции, в пределах которой транзакция была создана, обработана, выполнена и/или сохранена.

14.2 Безопасность процессов разработки и поддержки

Цель: Обеспечить разработку и внедрение информационной безопасности в течение всего жизненного цикла разработки информационных систем.

14.2.1 Политика безопасной разработки

Средство управления

Установление и применение правил по разработке программного обеспечения и систем, выполняемой организацией.

Руководство по внедрению

Обеспечение безопасной разработки требуется для создания безопасных сервисов, архитектуры, программного обеспечения и системы.

В политике безопасной разработки должны быть отражены следующие аспекты:

a) безопасность среды разработки;

b) руководство по безопасности в жизненном цикле разработки программного обеспечения:

1) безопасность в методологии разработки программного обеспечения;

2) рекомендации по безопасному кодированию для каждого используемого языка программирования;

c) требования безопасности на этапе проектирования;

d) контрольные точки управления безопасностью на этапах проектирования;

e) безопасные репозитории;

f) безопасность управления версиями;

g) необходимые знания о безопасности приложения;

h) наличие возможностей у разработчиков для предотвращения возникновения, обнаружения и фиксации уязвимостей.

В тех случаях, когда ничего не известно о стандартах, применяемых при разработке, или они не соответствуют современным лучшим практикам, следует использовать методы безопасного программирования как при выполнении новых разработок, так и при сценариях повторного использования кода. Следует учитывать требования стандартов кодирования и самые важные из них обязательно использовать. Разработчикам следует научиться использовать эти стандарты и проверять их использование посредством тестирования и анализа кода.

В том случае, когда разработка выполняется сторонней организацией, организация-заказчик должна убедиться в том, что в этой организации строго соблюдаются правила по безопасной разработке программного обеспечения и систем (14.2.7).

Дополнительная информация

Кроме того, может выполняться разработка внутренних приложений, например, таких как офисные приложения, сценарии, браузеры и базы данных.

14.2.2 Процедуры управления изменениями системы

Средство управления

Управление изменениями, вносимыми в системы в течение жизненного цикла их разработки, посредством использования формальных процедур управления изменениями.

Руководство по внедрению

Для обеспечения целостности системы, приложений и продуктов следует документировать и выполнять формальные процедуры управления изменениями еще на этапах проектирования и впоследствии на всех последующих этапах эксплуатации. Введение новых систем и внесение значительных изменений в существующие системы должно осуществляться посредством формального процесса документирования, спецификации, тестирования, контроля качества и управления реализацией.

Данный процесс должен включать определение рисков, анализ влияний изменений и спецификации необходимых средств управления безопасностью. Кроме того, данный процесс должен гарантировать, что существующие безопасность и процедуры управления не скомпрометированы, что осуществляющие поддержку программисты получат доступ только к тем частям системы, которые необходимы для их работы, и что для любого изменения будет получено формальное соглашение и утверждение.

При наличии возможности, процедуры управления изменениями прикладного и системного программного обеспечения должны быть объединены (12.1.2). Процедуры изменения должны включать, но не ограничиваться только этим:

a) протоколирование согласованных уровней полномочий;

b) обеспечение внесения изменений только полномочными пользователями;

c) анализ средств управления и процедур обеспечения целостности, который позволит удостовериться в том, что изменения не приведут к их компрометации;

d) идентификацию всего программного обеспечения, информации, объектов баз данных и аппаратных средств, которым требуются изменения;

e) идентификацию и проверку критичного для безопасности кода, чтобы минимизировать вероятность известных слабостей безопасности;

f) получение до начала работ формального одобрения детализированных предложений по изменениям;

g) обеспечение согласования предлагаемых изменений с полномочным пользователем до их непосредственной реализации;

h) обеспечение обновления комплекта системной документации после завершения каждого изменения и архивирование или утилизация старой документации;

i) поддержку управления версиями для всех обновлений программного обеспечения;

j) регистрацию в журналах аудита всех запросов на внесение изменений;

k) обеспечение коррекции эксплуатационной документации (12.1.1) и пользовательских процедур в соответствии с внесенными изменениями;

l) обеспечение того, чтобы внесение изменений происходило своевременно и не нарушало затрагиваемые бизнес-процессы.

Дополнительная информация

Изменение программного обеспечения может повлиять на среду эксплуатации и наоборот.

Хорошая практика предусматривает тестирование нового программного обеспечения в среде, отделенной от среды эксплуатации и от среды разработки (12.1.4). Данная практика позволяет осуществлять контроль над новым программным обеспечением и предоставляет дополнительную защиту эксплуатационной информации, используемой для тестирования. Оно должно включать тестирование программных заплаток, сервисных пакетов и прочие обновления.

При рассмотрении возможности автоматических обновлений следует сравнить преимущества быстрой установки обновлений с риском нарушения целостности и доступности системы, служебных пакетов и прочих обновлений. Не следует использовать автоматическое обновление в критических системах, поскольку некоторые обновления могут вызвать нарушение работы критических приложений.

14.2.3 Технический анализ приложений после изменений операционных платформ

Средство управления

Проведение анализа и тестирования критических бизнес-приложений при изменениях операционных платформ для обеспечения уверенности в том, что не будет оказано никакого отрицательного влияния на деятельность или безопасность организации.

Руководство по внедрению

Данный процесс должен учитывать:

a) анализ процедур управления и обеспечения целостности в приложениях, обеспечивающий уверенность в том, что они не были скомпрометированы при изменениях операционной платформы;

b) обеспечение заблаговременного поступления уведомлений об изменениях операционной платформы, чтобы стало возможным проведение надлежащего тестирования и анализа до ее реализации;

c) обеспечение внесения соответствующих изменений в планы обеспечения непрерывности бизнес-деятельности (раздел 17).

Дополнительная информация

Операционные платформы включают операционные системы, платформы баз данных и межплатформного программного обеспечения. Следует также контролировать изменения используемых приложений.

14.2.4 Ограничения на внесение изменений в пакеты программ

Средство управления

Ограничение модификаций пакетов программ только внесением необходимых изменений. Строгий контроль за всеми изменениями.

Руководство по внедрению

Насколько это возможно и применимо на практике, все предоставленные поставщиками пакеты программ должны использоваться без изменений. Если все же пакеты программ необходимо модифицировать, то надлежит рассмотреть следующие вопросы:

a) риск компрометации встроенных средств управления и процедур обеспечения целостности;

b) требуется ли получить разрешение поставщика;

c) возможность внесения требуемых изменений поставщиком в виде стандартных обновлений программы;

d) последствия в том случае, если в результате внесения изменений дальнейшая поддержка программного обеспечения становится обязанностью самой организации;

e) совместимость с другим используемым программным обеспечением.

Если изменения необходимы, следует сохранять исходное программное обеспечение и вносить изменения в четко определенную копию. Должен быть реализован процесс управления обновлением программного обеспечения, чтобы обеспечить установку для всего авторизованного программного обеспечения последних утвержденных исправлений и обновлений прикладных программ (12.6.1). Все изменения должны быть полностью протестированы и задокументированы, чтобы их можно было повторно внести при обновлении программного обеспечения в будущем. Если требуется, то изменения должны быть протестированы и оценены соответствующим независимым органом по сертификации.

14.2.5 Принципы разработки безопасных систем

Средство управления

Установление, документирование, поддержка и применение принципов разработки безопасных (защищенных) систем при внедрении любых информационных систем.

Руководство по внедрению

При разработке информационной системы организации следует установить, задокументировать и применять процедуры разработки

безопасных информационных систем, основанные на принципах обеспечения безопасности.

Безопасность следует проектировать на всех уровнях архитектуры (бизнес, данные, приложения и технологии), балансируя между потребностью в информационной безопасности и потребностью в доступности. Новые технологии следует анализировать относительно рисков безопасности, а проект - на предмет того, предусмотрена ли в нем защита от известных схем атак.

Эти установленные принципы и процедуры разработки безопасных систем следует периодически пересматривать, чтобы убедиться в том, что они:

a) эффективно содействуют внедрению современных стандартов по безопасности в процессе разработки систем;

b) на данный момент продолжают быть актуальными относительно противодействия любым новым потенциальным угрозам и продолжают применяться в предлагаемых прогрессивных технологиях и решениях.

Установленные принципы разработки безопасности, при необходимости, следует применять и к информационным системам сторонних организаций. Это достигается посредством контрактов и других обязательных соглашений между данной и сторонней организациями, когда последняя является провайдером услуг. Организация должна подтвердить строгое соответствие принципов разработки безопасности ее и провайдера услуг.

Дополнительная информация

В процедурах разработки приложений должны использоваться методы разработки безопасного программного обеспечения применительно к разработке приложений, у которых имеются входные и выходные интерфейсы. Методы разработки безопасного программного обеспечения представляют собой руководство по методам аутентификации пользователей, управлению сеансом засекреченной связи и проверке достоверности данных, поиску и исправлению ошибок в разрабатываемых программах.

14.2.6 Безопасная среда разработки

Средство управления

Установление и соответствующая защита организациями безопасных сред разработки систем и работ по их интеграции, которые охватывают весь жизненный цикл разработки системы.

Руководство по внедрению

Безопасная среда разработки включает персонал, процессы и технологию, связанные с разработкой и интеграцией системы.

При установлении безопасной среды разработки для специфических этапов разработки системы организации должны определить риски,

связанные с отдельными этапами разработки системы, с учетом следующих факторов:

a) чувствительности данных, которые должны обрабатываться, храниться и передаваться системой;

b) применяемых внешних и внутренних требований, например, из нормативно-правовых актов или политик;

c) средств управления безопасностью уже реализованных в организации, которая поддерживает разработку системы;

d) благонадежности персонала, работающего в безопасной среде (7.1.1);

e) степени делегирования сторонней организации работ, связанных с разработкой системы;

f) потребности в изоляции между различными средами разработки;

g) управления доступом к безопасной среде разработки;

h) мониторинга изменений в безопасной среде и хранящегося в ней кода;

i) хранения резервных копий в других безопасных помещениях;

j) управления перемещением данных из безопасной среды и обратно.

Как только для специфической среды разработки будет определен необходимый уровень защиты, организации должны подтвердить соответствие процессов в безопасных процедурах разработки и обеспечить ими всех тех отдельных сотрудников, которым они необходимы.

14.2.7 Разработка системы сторонней организацией

Средство управления

Осуществление организацией надзора и мониторинга деятельности по разработке системы, выполняемой сторонней организацией.

Руководство по внедрению

В тех случаях, когда для разработки системы привлекается сторонняя организация, надлежит одновременно рассмотреть всю внешнюю цепочку поставок организации и следующие вопросы:

a) лицензионные соглашения, собственность на код и права на интеллектуальную собственность, связанные с контентом (информационным наполнением) разработки, выполненной сторонней организацией (18.1.2);

b) договорные требования, устанавливающие правила по безопасному проектированию, кодированию и тестированию (14.2.1);

c) предоставление утвержденной модели угрозы внешнему разработчику;

d) приемо-сдаточное тестирование, выполняемое с целью проверки для качества и точности поставляемых конечных результатов разработки;

e) предоставление свидетельства того, что пороги безопасности были использованы для установления минимально допустимых уровней безопасности и качества обеспечения приватности;

f) предоставление свидетельства того, что было выполнено надлежащее тестирование, гарантирующее отсутствие как преднамеренно, так и непреднамеренно внесенного вредоносного содержимого в поставляемых конечных результатах разработки;

g) предоставление свидетельства того, что было выполнено надлежащее тестирование, гарантирующее отсутствие известных уязвимостей;

h) соглашение о депонировании, предусматривающее, например, тот случай, когда исходный код будет недоступным;

i) предусмотренное договором право проводить аудит процессов разработки и средств управления;

j) утвержденная документация по созданию среды сборки, использованной при завершении разработки;

k) ответственность организации за соответствие действующему законодательству и проверку эффективности управления.

14.2.8 Тестирование безопасности системы

Средство управления

Выполнение тестирования функциональных возможностей безопасности в процессе разработки.

Руководство по внедрению

Новые и модернизированные системы необходимо тщательно тестировать и проверять в процессе разработки, также необходимо составить подробный календарный план работ, описать входные и предполагаемые выходные тестовые данные в соответствующем диапазоне условий. При разработке, выполняемой самой организацией, первоначально эти тесты должна выполнить группа разработчиков. Далее должно произойти независимое приемо-сдаточное тестирование (разработок, выполненных как самой, так и сторонней организацией), позволяющее убедиться в том, что система работает как предполагалось и только как предполагалось (14.1.1 и 14.2.9). Объем тестирования должен соизмеряться с важностью и природой системы.

14.2.9 Приемо-сдаточное тестирование системы

Средство управления

Разработка программ приемо-сдаточного тестирования для новых и модернизированных систем, а также для новых версий программного обеспечения и определение соответствующих критериев.

Руководство по внедрению

Приемо-сдаточное тестирование систем должно включать тестирование по требованиям информационной безопасности (14.1.1 и 14.1.2) и проверку соблюдения правил разработки безопасных систем (14.2.1). Кроме того, должно быть проведено тестирование полученных компонентов и интегрированных систем. Организации должны проверить устранение дефектов, связанных с безопасностью, для этого они могут

использовать автоматизированные инструментальные средства, например, анализаторы кодов или сканеры уязвимостей.

Тестирование должно выполняться в реальной среде тестирования, позволяющей проверить, что новая система не внесет дополнительных уязвимостей в среду эксплуатации организации, а также проверить надежность тестов.

14.3 Тестовые данные

Цель: Обеспечить защиту данных, используемых для тестирования.

14.3.1 Защита тестовых данных

Средство управления

Тщательный выбор, защита и контроль тестовых данных.

Руководство по внедрению

Следует избегать использования рабочих данных, содержащих персональные данные, идентифицирующие личность, или другую конфиденциальную информацию, для целей тестирования. Если персональные данные или другая конфиденциальная информация используется для целей тестирования, то перед ее использованием все конфиденциальные сведения и содержимое должны быть удалены или изменены таким образом, чтобы невозможно было их опознать.

Для защиты рабочих данных, используемых для целей тестирования, следует выполнять следующие рекомендации:

a) процедуры управления доступом, применяемые в рабочих прикладных системах, следует также применять и для тестовых прикладных систем;

b) на каждое копирование рабочей информации в среду тестирования следует получать специальное разрешение;

c) после завершения тестирования, рабочую информацию следует немедленно удалить из среды тестирования;

d) сведения о копировании и использовании рабочей информации следует регистрировать в журнале аудита.

Дополнительная информация

Системное и приемо-сдаточное тестирование обычно требуют использования существенного объема тестовых данных, которые максимально приближены к рабочим данным.

15 Взаимоотношения с поставщиками

15.1 Информационная безопасность при взаимоотношениях с поставщиками

Цель: Обеспечить защиту активов организации, к которым имеют доступ поставщики.

15.1.1 Политика информационной безопасности в области взаимоотношений с поставщиками

Средство управления

Согласование с поставщиками и документирование требований информационной безопасности, позволяющих минимизировать риски, связанные с доступом поставщиков к активам организации.

Руководство по внедрению

Организация должна определить и обязательно внедрить средства управления информационной безопасностью, в связи с этим в политике необходимо рассмотреть вопрос относительно доступа поставщика к информации организации. Средства управления, адресованные процессам и процедурам, которые следует внедрить в организации, а также тем процессам и процедурам, внедрения которых организация должна потребовать у поставщика, включают:

a) идентификацию и документирование типов поставщиков, например, поставщики сервисов ИТ, логистических утилит, финансовых сервисов, компонентов инфраструктуры ИТ, которым организация выдает разрешение на доступ к своей информации;

b) стандартный процесс и жизненный цикл для управления отношениями с поставщиком;

c) определение типов доступа к информации, который будет разрешен различным типам поставщиков, а также мониторинг и управление доступом;

d) минимальные требования информационной безопасности для каждого типа информации и типа доступа, которые будут служить основой для соглашений с отдельными поставщиками, основанные на потребностях и требованиях бизнеса организации, а также на ее профиле рисков;

e) процессы и процедуры по мониторингу строгого соблюдения установленных требований информационной безопасности для каждого типа поставщика и типа доступа, в том числе анализ и оценка качества продукта третьей стороной;

f) точность и полноту средств управления, обеспечивающих целостность информации или выполняющих обработку информации, принадлежащих любой из сторон;

g) типы соглашений с поставщиками по защите информации организации;

h) обработку инцидентов и внештатных ситуаций, связанных с доступом поставщика, включая ответственность как организации, так и поставщиков;

i) способность системы к восстановлению функций и, при необходимости, планы обеспечения непрерывной работы и восстановления, обеспечивающие доступность информации или выполнения обработки информации любой из сторон;

j) проведение тренингов для персонала организации по повышению его осведомленности относительно применяемых политик, процессов и процедур;

k) проведение тренингов для персонала организации, взаимодействующего с персоналом поставщика, по повышению его осведомленности относительно установленных правил взаимодействия с поставщиками и стиля поведения в зависимости от типа поставщика и уровня доступа поставщика к системам и информации организации;

l) условия, при выполнении которых требования информационной безопасности и средства управления будут зафиксированы в соглашении, подписанном обеими сторонами;

m) руководство необходимой поставкой информации, средств обработки информации и другого, что должно быть поставлено, и обеспечением информационной безопасности в течение всего периода поставки.

Дополнительная информация

Информация организации может быть подвержена риску нарушения безопасности при доступе поставщиков из-за неадекватного управления безопасностью. Следует установить и применить средства управления по администрированию доступа поставщиков к средствам обработки информации. Например, если существует особая потребность в обеспечении конфиденциальности информации, то можно заключить соглашение о ее неразглашении. Следующим примером рисков является несоблюдение требований по защите данных, когда в соглашении с поставщиком оговорены трансграничная передача информации или трансграничный доступ к информации. Организация должна знать об ответственности за защиту информации, возлагаемой на нее законодательством или договором.

15.1.2 Соглашения с поставщиками по информационной безопасности

Средство управления

Установление всех надлежащих требований информационной безопасности и согласование их с каждым поставщиком, который может иметь доступ к информации организации и процессам управления

данными, хранить и передавать информацию или поставлять компоненты инфраструктуры ИТ для организации.

Руководство по внедрению

Для исключения возможности неверного истолкования взаимных обязательств организации и поставщика относительно выполнения надлежащих требований информационной безопасности следует установить и задокументировать соответствующие соглашения с поставщиками.

Для удовлетворения установленных требований по информационной безопасности в соглашениях должны быть отражены следующие условия:

a) описание предоставляемой или доступной информации, либо описание методов предоставления информации или предоставления к ней доступа;

b) классификация информации в соответствии с системой классификации, принятой в организации (8.2); при необходимости также установление соответствия между системами классификации информации организации и поставщика;

c) требования законодательных и нормативно-правовых актов по защите данных, прав на интеллектуальную собственность и авторского права, а также описание того, как будет выполняться проверка удовлетворения этих требований;

d) обязательство каждой из договаривающихся сторон осуществлять согласованную установку средств управления, в том числе по управлению доступом, аттестации, мониторингу, отчетности и аудиту;

e) правила допустимого использования информации, в том числе, при необходимости, правила недопустимого ее использования;

f) список персонала поставщика, уполномоченного получать доступ к информации или получать информацию от организации, либо процедуры или условия выполнения и прекращения авторизации для доступа к информации или получения информации от организации персоналом поставщика;

g) политики информационной безопасности, важные для конкретного соглашения;

h) требования и процедуры по управлению инцидентами (особенно в части оповещения и взаимодействия во время ликвидации последствий инцидента);

i) требования по проведению тренингов и обеспечению осведомленности о конкретных процедурах и требованиях информационной безопасности, например, по процедурам реагирования, процедурам авторизации;

j) соответствующие инструкции для субпоставщиков с описанием средств управления, которые должны быть внедрены;

k) соответствующие стороны соглашения, в том числе контактное лицо по вопросам информационной безопасности;

l) требования по отбору персонала поставщика, при необходимости, в том числе ответственность за проведение отбора и процедуры уведомления, если отбор не завершен или его результаты являются причиной для сомнений или беспокойства;

m) право на аудит процессов и средств управления поставщика, имеющих отношение к соглашению;

n) процессы обнаружения и устранения дефектов;

o) обязательство поставщика периодически предоставлять независимый отчет об эффективности средств управления и договор о своевременной коррекции важных вопросов, поднятых в отчете;

p) обязательства поставщика по соблюдению требований по безопасности организации.

Дополнительная информация

Соглашения могут значительно различаться для разных организаций и для различных типов поставщиков. Таким образом, следует позаботиться о включении в соглашения всех соответствующих рисков и требований информационной безопасности. В соглашения с поставщиками также могут быть включены и другие стороны (например, субпоставщики).

В соглашении должны быть рассмотрены процедуры для продолжения обработки информации в том случае, если поставщик окажется не в состоянии предоставлять свои продукты или сервисы, чтобы избежать каких-либо задержек в обеспечении замены этих продуктов или сервисов.

15.1.3 Цепочки поставок информационно-коммуникационных технологий

Средство управления

Включение в соглашения с поставщиками требований по учету рисков информационной безопасности, связанных с цепочками поставок сервисов и продуктов информационно-коммуникационных технологий (ИКТ).

Руководство по внедрению

Для обеспечения безопасности цепочки поставки в соглашения с поставщиками следует включить следующие вопросы:

a) определение требований информационной безопасности к закупке продукта или сервиса ИКТ, дополняющих общие требования информационной безопасности при взаимоотношениях с поставщиками;

b) распространение поставщиками сервисов ИКТ требований по безопасности организации по всей цепочке поставки, если было предусмотрено, что частичная поставка сервисов ИКТ для организации будет осуществляться субпоставщиками;

c) распространение поставщиками продуктов ИКТ соответствующих методов безопасности по всей цепочке поставки, если эти продукты включают компоненты, приобретаемые у других поставщиков;

d) внедрение процесса мониторинга и надлежащих методов для подтверждения того, что данные продукты и сервисы ИКТ удовлетворяют установленным требованиям по безопасности;

e) внедрение процесса определения компонентов продукта или сервиса, критичных для поддержки функциональных возможностей и, следовательно, требующих повышенного внимания и изучения, если они были скомпонованы за пределами организации и, особенно, если ведущий поставщик привлек к поставке продукта или сервиса других поставщиков;

f) получение уверенности в том, что может быть отслежена вся цепочка поставки критических компонентов и их производителей;

g) получение уверенности в том, что поставленные продукты ИКТ функционируют должным образом и что у них отсутствуют какие-либо непредусмотренные или нежелательные характеристики;

h) определение правил совместного использования информации относительно цепочки поставки и любых других, возможно возникающих вопросов и соглашений между организацией и поставщиками;

i) реализация конкретных процессов управления жизненным циклом и доступностью компонентов ИКТ, а также соответствующими рисками информационной безопасности. При управлении рисками компонентов следует предусмотреть устаревание компонентов: они могут стать более недоступны из-за поставщиков или перестанут более использоваться в бизнесе, или же поставщики более не будут поставлять эти компоненты вследствие снятия их с производства из-за изменения технологии.

Дополнительная информация

Методы управления рисками в цепочке поставок конкретных ИКТ дополняют общее управление информационной безопасностью, качеством, проектами и методы системной инженерии, но не заменяют их.

Организациям, которые работают с поставщиками, рекомендуется ознакомиться с цепочкой поставок ИКТ и любых материалов, которые оказывают существенное влияние на предоставление продуктов и сервисов. Организации могут повлиять на цепочку поставок ИКТ, включая в соглашения с их поставщиками требования информационной безопасности, которые, в свою очередь, следует адресовать своим субпоставщикам в этой цепочке поставок ИКТ.

Рассмотренная в настоящем стандарте цепочка поставок ИКТ включает сервисы «облачных» вычислений.

15.2 Управление сервисами, предоставляемыми поставщиками

Цель: Поддерживать уровни информационной безопасности и предоставляемых сервисов, установленные в соглашениях с поставщиками.

15.2.1 Мониторинг и анализ сервисов, предоставляемых поставщиками

Средство управления

Регулярное осуществление организациями мониторинга, анализа и аудита сервисов, предоставляемых поставщиком.

Руководство по внедрению

Мониторинг и анализ сервисов, предоставляемых поставщиком, должны обеспечивать соблюдение условий соглашений, относящихся к информационной безопасности, а также должное управление инцидентами и проблемами информационной безопасности.

Сюда же следует включить следующие вопросы взаимодействия между организацией и поставщиком при управлении сервисами:

a) мониторинг уровней производительности сервисов для подтверждения соблюдения соглашений;

b) анализ отчетов по сервисам, подготовленных поставщиком, а также организация регулярных совещаний по вопросу хода работ в соответствии с соглашениями;

c) проведение аудита поставщиков одновременно с анализом отчетов независимых аудиторов, при наличии, и проверка выполнения определенных вопросов;

d) предоставление информации об инцидентах информационной безопасности, а также анализ этой информации в соответствии с соглашениями и другими вспомогательными рекомендациями и процедурами;

e) анализ журналов аудитов поставщика и записей о событиях информационной безопасности, эксплуатационных проблемах, неисправностях, трассировки отказов и нарушений, относящихся к предоставляемым сервисам;

f) решение и управление любыми возникающими проблемами;

g) анализ аспектов информационной безопасности во взаимоотношениях поставщика с его субпоставщиками;

h) обеспечение поставщиком поддержки достаточных возможностей сервисов вместе с реальными планами, разработанными с целью обеспечения согласованных уровней бесперебойности сервисов и восстановления предоставления основных сервисов после сбоев или чрезвычайных ситуаций (раздел 17).

Ответственность за управление взаимоотношениями с поставщиком должна быть возложена на конкретное лицо или группу по управлению

сервисами. Кроме того, организации следует убедиться в том, что поставщики назначили ответственных за проверку соответствия и выполнения требований соглашений. Для контроля выполнения требований соглашения, в особенности, требований информационной безопасности, следует выделить персонал, обладающий достаточными техническими навыками, и достаточное количество ресурсов. При обнаружении недостатков в предоставляемых сервисах следует принимать надлежащие меры.

Организация должна поддерживать адекватный общий контроль и наблюдение за всеми аспектами безопасности чувствительной или критичной информации или средств обработки информации, к которым поставщик имеет доступ, использует для обработки или которыми управляет. Организация должна обеспечить наблюдение за деятельностью, связанной с безопасностью, например, за внесением изменений, идентификацией уязвимостей и уведомлением/реагированием в случае инцидентов информационной безопасности, посредством четко определенной процедуры предоставления отчетности.

15.2.2 Управление внесением изменений в сервисы, предоставляемые поставщиками

Средство управления

Управление внесением изменений в предоставляемые сервисы, в том числе поддержка и совершенствование существующих политик информационной безопасности, процедур и средств управления с учетом критичности задействованных бизнес-информации, бизнес-процессов и систем, а также последующее повторное определение рисков.

Руководство по внедрению

Следует принять во внимание нижеперечисленные аспекты:

a) внесение изменений в соглашения с поставщиками;

b) внесенные организацией изменения для реализации:

1) улучшений в предоставляемых сервисах;

2) разработки каких-либо новых приложений и систем;

3) модификации или обновления политик и процедур, принятых в организации;

4) новых или замененных средств управления для разрешения инцидентов информационной безопасности и для повышения уровня безопасности;

c) изменения в сервисах поставщика, реализующие:

1) изменения и улучшения в сетях;

2) использование новых технологий;

3) внедрение новых программных продуктов или новых версий/релизов;

4) новые инструментальные средства и среды разработки;

5) изменения в физическом местоположении сервисных технических средств;

6) смена поставщиков;

7) заключение субподрядного договора с другим поставщиком.

16 Управление инцидентами информационной безопасности

16.1 Управление инцидентами информационной безопасности и его улучшение

Цель: Обеспечить применение последовательного и эффективного подхода к управлению инцидентами информационной безопасности, в том числе к обмену информацией о событиях и недостатках безопасности.

16.1.1 Ответственность и процедуры

Средство управления

Определение ответственности руководства и процедур по управлению инцидентами информационной безопасности, обеспечивающих быстрое, эффективное и организованное реагирование на эти инциденты.

Руководство по внедрению

Следует принять во внимание следующие рекомендации об ответственности руководства и о процедурах по управлению инцидентами информационной безопасности:

a) определить ответственность руководства за разработку нижеперечисленных процедур и информирование о них надлежащим образом соответствующих категорий персонала организации:

1) процедуры планирования и подготовки реагирования на инциденты;

2) процедуры мониторинга, обнаружения, анализа и отчетности событий и инцидентов информационной безопасности;

3) процедуры регистрации деятельности по управлению инцидентами;

4) процедуры обработки свидетельств, необходимых для судебных разбирательств;

5) процедуры обнаружения событий информационной безопасности и принятия решений по ним, а также процедуры обнаружения недостатков информационной безопасности;

6) процедуры реагирования на инциденты информационной безопасности, включающие эскалацию (т.е. передачу управления инцидентом вышестоящему уполномоченному лицу), управляемого восстановления после инцидента и оповещения соответствующих должностных лиц своей организации или сторонних организаций;

b) определенные процедуры должны обеспечивать, чтобы:

1) вопросами, относящимися к инцидентам информационной безопасности, занимался компетентный персонал организации;

2) была создана контактная позиция по обнаружению инцидентов безопасности и отчетности;

3) поддерживались соответствующие контакты с авторитетными специалистами, внешними группами по интересам или форумами, которые рассматривают вопросы, относящиеся к инцидентам информационной безопасности;

c) процедуры оповещения должны включать:

1) подготовку формы отчета о событии информационной безопасности, которая поможет подотчетному лицу при составлении отчета вспомнить все выполненные действия при наступлении события информационной безопасности;

2) процедуры, которые следует предпринять в случае наступления события информационной безопасности, например, немедленно отмечать все подробности, такие как тип несоответствия или нарушения, возникающий сбой, сообщения на экране, немедленно оповещать контактную позицию и выполнять только скоординированные действия;

3) ссылка на установленный официальный дисциплинарный процесс для работы с тем персоналом, который нарушает безопасность;

4) соответствующие процедуры обратной связи, обеспечивающие информирование лиц, сообщивших о событиях информационной безопасности, о результатах после разрешения и закрытия вопроса.

Цели управления инцидентами информационной безопасности должны быть согласованы с руководством, также следует обеспечить, чтобы сотрудники, ответственные за управление инцидентами информационной безопасности, понимали принятые в организации приоритеты в плане урегулирования инцидентов информационной безопасности.

Дополнительная информация

Инциденты информационной безопасности могут выходить за пределы организации и за границы страны. Для реагирования на подобные инциденты в некоторых ситуациях существует все возрастающая потребность в координации ответных действий и совместном использовании информации об этих инцидентах с внешними организациями.

Подробное руководство по управлению инцидентами информационной безопасности приведено в O‘z DSt ISO/IEC 27035.

16.1.2 Оповещение о событиях информационной безопасности

Средство управления

Незамедлительное, насколько это возможно, оповещение руководства о событиях информационной безопасности по соответствующим каналам.

Руководство по внедрению

Весь персонал и все работающие по договору должны быть осведомлены об их ответственности за незамедлительное оповещение о событиях информационной безопасности. Они также должны быть осведомлены о процедурах отчетности и о контактной позиции, куда следует предоставлять отчеты о событиях информационной безопасности.

Ситуации, на которые следует обратить внимание при составлении отчета о событии информационной безопасности, включают:

a) неэффективное управление безопасностью;

b) предполагаемое нарушение целостности, конфиденциальности или доступности информации;

c) ошибки, связанные с человеческим фактором;

d) несоответствие политикам или рекомендациям;

e) нарушения мер физической безопасности;

f) неконтролируемые системные изменения;

g) сбои программного обеспечения или аппаратных средств;

h) нарушение прав доступа.

Дополнительная информация

Нарушения работы или другое аномальное поведение системы может служить индикатором атаки, угрожающей безопасности, или фактического нарушения безопасности, так что об этом всегда нужно оповещать как о событии информационной безопасности.

16.1.3 Оповещение о недостатках информационной безопасности

Средство управления

Предъявление требования ко всему персоналу и всем работающим по договору о необходимости отмечать и сообщать о любых наблюдаемых или предполагаемых недостатках безопасности в системах или сервисах.

Руководство по внедрению

Всему персоналу и всем работающим по договору следует незамедлительно предоставлять эти материалы контактной позиции для предотвращения инцидентов информационной безопасности. Механизм оповещения должен быть как можно более легким, понятным и доступным.

Дополнительная информация

Весь персонал и все работающие по договору должны быть осведомлены о недопустимости их самостоятельных попыток доказать наличие предполагаемых недостатков безопасности. Тестирование недостатков может быть интерпретировано как потенциальное неправомерное использование системы, оно способно также вызвать повреждение информационной системы или сервиса и привести к юридической ответственности лица, самовольно выполнившего тестирование.

16.1.4 Оценка событий информационной безопасности и принятие решений

Средство управления

Оценка событий информационной безопасности и принятие решения о том, следует ли их классифицировать как инциденты информационной безопасности.

Руководство по внедрению

Контактная позиция должна оценить каждое событие информационной безопасности, используя согласованную классификационную шкалу событий и инцидентов информационной безопасности, а также принять решение, следует ли классифицировать это событие как инцидент информационной безопасности. Классификация и категоризация инцидентов могут помочь при идентификации влияния и длительности инцидента.

В тех случаях, когда в организации имеется Служба реагирования на инциденты информационной безопасности (СРИИБ), то вышеуказанные оценка и решение могут быть направлены в СРИИБ для подтверждения или переоценки.

Результаты оценки и решение следует записывать настолько подробно, чтобы впоследствии их можно было использовать для ссылок и при проверках.

16.1.5 Реагирование на инциденты информационной безопасности

Средство управления

Реагирование на инциденты информационной безопасности в соответствии с документированными процедурами.

Руководство по внедрению

На инциденты информационной безопасности должны реагировать назначенная контактная позиция и другие соответствующие должностные лица организации или сторонних организаций (16.1.1).

Процесс реагирования на инциденты должен включать:

a) незамедлительный, насколько это возможно, сбор свидетельств после случившегося события или инцидента информационной безопасности;

b) проведение экспертного анализа информационной безопасности, при необходимости (16.1.7);

c) эскалацию, при необходимости;

d) обеспечение в установленном порядке регистрации деятельности по реагированию, которая потребуется для последующего анализа;

e) информирование о наличии инцидента информационной безопасности или любых относящихся к нему данных других внутренних и внешних лиц или организаций, которым это положено знать;

f) обнаружение недостатка(ов) информационной безопасности, явившегося причиной инцидента или содействующего его возникновению;

g) официальное закрытие и регистрацию инцидента после его успешного устранения.

После устранения инцидента для определения его источника, при необходимости, следует произвести соответствующий анализ.

Дополнительная информация

Первоначальной целью реагирования на инциденты является возобновление «нормального уровня безопасности», а затем выполнение необходимого восстановления.

16.1.6 Изучение инцидентов информационной безопасности

Средство управления

Использование знаний, полученных при выполнении анализа и устранении инцидентов информационной безопасности, для уменьшения вероятности возникновения или влияния будущих инцидентов.

Руководство по внедрению

Следует установить механизмы, позволяющие осуществлять оценку и мониторинг количества, типов, параметров инцидентов информационной безопасности, а также связанных с ними затрат. Информацию, полученную в результате оценки инцидентов информационной безопасности, следует использовать для определения повторных инцидентов или инцидентов, наносящих серьезный ущерб.

Дополнительная информация

Оценка инцидентов информационной безопасности может указывать на необходимость совершенствования или введения дополнительных средств управления с целью минимизации частоты возникновения таких инцидентов в будущем, а также величины связанных с ними ущерба и затрат. Кроме того, эту оценку следует учитывать при пересмотре политики безопасности (5.1.2).

При соблюдении конфиденциальности надлежащим образом, случаи имевших место реальных инцидентов информационной безопасности могут быть использованы на тренингах по повышению осведомленности пользователей (7.2.2) в качестве примеров возможных инцидентов, при этом следует рассмотреть способы реагирования на такие инциденты и предотвращения возникновения их в будущем.

16.1.7 Сбор свидетельств

Средство управления

Определение и применение процедур идентификации, сбора, получения и хранения информации, которая может служить в качестве свидетельства.

Руководство по внедрению

Следует разработать и соблюдать внутренние процедуры изучения свидетельств в целях принятия дисциплинарных и законодательных мер.

Как правило, эти процедуры должны обеспечить процессы идентификации, сбора, получения и хранения свидетельства в соответствии с различными типами носителей, устройств и в зависимости от того, в каком состоянии эти устройства находятся, например, во включенном или выключенном. В этих процедурах должно быть учтено следующее:

a) порядок передачи и хранения;

b) безопасность свидетельства;

c) безопасность персонала;

d) задействованные роли и ответственность персонала;

e) компетенция персонала;

f) документация;

g) брифинг.

Для достижения приемлемости хранимого свидетельства следует затребовать сертификаты или другие соответствующие документы, подтверждающие квалификацию персонала, а также сертификаты соответствия инструментальных средств, если таковые имеются.

Свидетельство, необходимое для судебных разбирательств, может находиться за пределами организации и/или юрисдикции. В этих случаях необходимо обеспечить, чтобы организации были предоставлены полномочия по сбору требуемой информации в качестве свидетельства. Следует также принимать во внимание требования в различных юрисдикциях, чтобы максимально повысить шансы на получение разрешения в соответствующей юрисдикции.

Дополнительная информация

Идентификация - это процесс, включающий поиск, распознавание и документирование потенциальных свидетельств. Сбор - это процесс сбора физических элементов, которые содержат потенциальные свидетельства. Получение - это процесс создания копии данных в пределах определенной совокупности. Хранение - это процесс поддержки и обеспечения целостности и исходного состояния потенциального свидетельства.

При обнаружении случившегося впервые события информационной безопасности может оказаться неочевидным, потребует ли оно судебного разбирательства. Таким образом, существует опасность, что необходимые свидетельства будут умышленно или случайно уничтожены прежде, чем будет осознана серьезность инцидента. В случае предполагаемых судебных разбирательств рекомендуется на самом раннем этапе обнаружения инцидента обратиться к юристу или в правоохранительные органы и получить консультацию относительно необходимых свидетельств.

17 Аспекты информационной безопасности при управлении непрерывностью бизнеса

17.1 Непрерывность информационной безопасности

Цель: Интегрировать непрерывность информационной безопасности в систему управления непрерывностью бизнеса организации.

17.1.1 Планирование непрерывности информационной безопасности

Средство управления

Определение организацией своих требований информационной безопасности и мероприятий по управлению непрерывностью информационной безопасности в нештатных ситуациях, например, в период кризиса или чрезвычайных ситуаций.

Руководство по внедрению

Организация должна определить, будет ли обеспечиваться непрерывность информационной безопасности в процессе управления непрерывностью бизнеса или в процессе управления восстановлением после чрезвычайных ситуаций. Требования информационной безопасности следует определить при планировании непрерывности бизнеса и восстановления после чрезвычайных ситуаций.

При отсутствии надлежаще оформленного планирования непрерывности бизнеса и восстановления после чрезвычайных ситуаций следует предположить, что к информационной безопасности в условиях нештатных ситуаций предъявляются те же самые требования, что и в штатном режиме. Кроме того, чтобы определить требования информационной безопасности применительно к нештатным ситуациям, организация может выполнить анализ воздействия аспектов информационной безопасности на бизнес.

Дополнительная информация

Для сокращения затрат времени и уменьшения объема работ при выполнении «дополнительного» анализа воздействия информационной безопасности на бизнес рекомендуется рассматривать аспекты информационной безопасности в штатном режиме управления непрерывностью бизнеса или при анализе воздействия на бизнес управления восстановлением после чрезвычайных ситуаций. При этом подразумевается, что требования к непрерывности информационной безопасности в явном виде сформулированы в процессе управления непрерывностью бизнеса или в процессе управления восстановлением после чрезвычайных ситуаций.

Более подробная информация об управлении непрерывностью бизнеса приведена в O‘z DSt ISO/IEC 27031.

17.1.2 Внедрение непрерывности информационной безопасности

Средство управления

Установление, документирование, внедрение и поддержка процессов, процедур и средств управления для обеспечения необходимого уровня непрерывности информационной безопасности в организации в нештатных ситуациях.

Руководство по внедрению

Организация должна обеспечить:

a) подготовку соответствующей структуры управления, предназначенной для реагирования и смягчения последствий разрушительных событий, из персонала, имеющего необходимые полномочия, опыт и компетентность;

b) назначение персонала, ответственного за реагирование на инциденты, имеющего необходимые полномочия и компетентность для управления инцидентами и поддержки информационной безопасности;

c) разработку и утверждение документированных планов, процедур реагирования и восстановления, описывающих подробно как организация в случае разрушительного события будет осуществлять управление и поддержку своей информационной безопасностью на предопределенном уровне, основанном на утвержденных целях управления непрерывностью информационной безопасности (17.1.1).

Согласно требованиям к непрерывности информационной безопасности, организация должна установить, задокументировать, внедрить и поддерживать:

a) средства управления информационной безопасностью в процесс обеспечения непрерывностью бизнеса или в процесс, процедуры восстановления после чрезвычайных ситуаций, а также вспомогательные системы и инструментальные средства;

b) процессы, процедуры и изменения реализации, необходимые для поддержки существующих средств управления информационной безопасностью в период нештатных ситуаций;

c) компенсирующие средства управления для тех средств управления информационной безопасностью, которые не могут быть задействованы в период нештатных ситуаций.

Дополнительная информация

В контексте непрерывности бизнеса или восстановления после чрезвычайных ситуаций могут быть определены конкретные процессы и процедуры. Информация, которая обрабатывается при выполнении этих процессов и процедур или в поддерживающих их специализированных информационных системах, должна быть защищена. Следовательно, организация должна привлечь специалистов по информационной безопасности к установлению, внедрению и поддержке процессов и процедур по обеспечению непрерывности бизнеса или восстановлению после чрезвычайных ситуаций.

Внедренные средства управления информационной безопасностью должны непрерывно функционировать в период нештатных ситуаций. Если средства управления не способны непрерывно обеспечивать информационную безопасность, то следует установить, внедрить и поддерживать другие средства управления, которые будут обеспечивать приемлемый уровень информационной безопасности.

17.1.3 Верификация, анализ и оценка непрерывности информационной безопасности

Средство управления

Регулярная верификация установленных и внедренных средств управления непрерывностью информационной безопасности для удостоверения в том, что они будут эффективно функционировать в период нештатных ситуаций.

Руководство по внедрению

Изменения в организационных, технических процедурах и процессах в контексте функционирования или обеспечения непрерывности могут стать причиной изменений требований к непрерывности информационной безопасности. В этих случаях должны быть приведены в соответствие с изменившимися требованиями процессы, процедуры и средства управления непрерывностью информационной безопасности.

Организации должны верифицировать свое управление непрерывностью информационной безопасности путем:

a) тренировок и тестирования функциональных возможностей процессов, процедур и средств управления непрерывностью информационной безопасности, чтобы удостовериться в том, что они соответствуют целям обеспечения непрерывности информационной безопасности;

b) тренировок и тестирования навыков и порядка выполнения процессов, процедур и средств управления непрерывностью информационной безопасности, чтобы удостовериться в том, что их выполнение соответствует целям обеспечения непрерывности информационной безопасности;

c) анализа достоверности и эффективности мер обеспечения непрерывности информационной безопасности при изменениях информационных систем, процессов, процедур и средств управления информационной безопасностью или процессов управления непрерывностью бизнеса/управления восстановлением после чрезвычайных ситуаций и решения.

Дополнительная информация

Верификация средств управления непрерывностью информационной безопасности отличается от тестирования и верификации общей информационной безопасности и должна выполняться отдельно от тестирования изменений. Если это возможно, более предпочтительным вариантом будет интеграция верификации средств управления

непрерывностью информационной безопасности с тестами на непрерывность бизнеса или тестами на восстановление после чрезвычайных ситуаций.

17.2 Резервирование

Цель: Обеспечить доступность средств обработки информации.

17.2.1 Доступность средств обработки информации

Средство управления

Внедрение средств обработки информации с достаточной степенью резервирования для удовлетворения требований к доступности.

Руководство по внедрению

Организации должны определить требования бизнеса к доступности информационных систем. Если существующая архитектура используемых систем не позволяет обеспечить доступность, следует предусмотреть резервные элементы или соответствующую архитектуру.

Если резервирование предусмотрено, резервные информационные системы следует протестировать, чтобы обеспечить автоматическое переключение одного элемента на другой элемент, работающий в штатном режиме.

Дополнительная информация

Внедрение резервирования может приводить к возникновению дополнительных рисков нарушения целостности или конфиденциальности информации и информационных систем, которые необходимо учитывать при проектировании информационных систем.

18 Соответствие требованиям

18.1 Соответствие требованиям законодательства и договоров

Цель: Избежать нарушений требований законодательства, нормативно-правовых актов или договорных обязательств, относящихся к информационной безопасности и любым требованиям безопасности.

18.1.1 Определение требований действующего законодательства и договоров

Средство управления

Четкое определение, документирование и поддержка в соответствии с текущим состоянием дел всех имеющих отношение к каждой информационной системе и организации требований законодательства,

нормативно-правовых актов и договоров, а также принятого в организации подхода к выполнению этих требований.

Руководство по внедрению

Следует также соответствующим образом определить и документировать конкретные средства управления и персональную ответственность должностных лиц за соблюдение этих требований.

Руководители должны определить все законодательство, применимое к их организации, для удовлетворения требований их бизнеса. Если организация ведет бизнес в других странах, то в этом случае необходимо учитывать требования законодательства этих стран.

18.1.2 Права на интеллектуальную собственность

Средство управления

Внедрение процедур, обеспечивающих соответствие требованиям законодательства, нормативно-правовых актов и договоров в области прав на интеллектуальную собственность, а также в области использования лицензионного программного обеспечения.

Руководство по внедрению

Для защиты любого материала, который может рассматриваться как интеллектуальная собственность, следует принять во внимание следующие рекомендации:

a) публикация политики соблюдения прав на интеллектуальную собственность, определяющей законное использование программного обеспечения и информационных продуктов;

b) приобретение программного обеспечения только через известные и имеющие хорошую репутацию источники для обеспечения гарантий того, что авторские права не нарушены;

c) поддержание осведомленности о политиках по защите прав на интеллектуальную собственность и уведомление о намерении применять дисциплинарные взыскания к тем сотрудникам, которые их нарушают;

d) поддержание соответствующих реестров ресурсов и определение всех ресурсов, для которых имеют место требования защиты прав интеллектуальной собственности;

e) сохранение подтверждений и свидетельств прав владения лицензиями, дистрибутивными дисками, руководства и т. п.;

f) реализация средств управления, которые обеспечивают соблюдение ограничения максимального числа разрешенных пользователей программного продукта;

g) выполнение проверок, гарантирующих установку только разрешенных и лицензированных программных продуктов;

h) обеспечение политики по соблюдению соответствующих условий лицензии;

i) обеспечение политики по утилизации или передаче программного обеспечения другим организациям;

j) соблюдение положений и условий для программного обеспечения и информации, полученных из сетей общего пользования;

k) не допускается дублирование, преобразование в другой формат или извлечение фрагментов коммерческих записей (видео, аудио) за исключением случаев, разрешенных законами об авторском праве;

l) не допускается полное или частичное копирование книг, статей, отчетов или других документов за исключением случаев, разрешенных законами об авторском праве.

Дополнительная информация

Права на интеллектуальную собственность включают в себя авторское право на программное обеспечение или документы, права на дизайн, торговые марки, патентные права и лицензии на исходные коды.

Лицензионные программные продукты обычно поставляются в рамках лицензионного соглашения, в котором определены условия лицензии, например, разрешение на использование программных продуктов только на определенных компьютерах или ограничение копирования только созданием резервных копий. Персонал организации должен быть проинформирован о наличии прав на интеллектуальную собственность на программное обеспечение, разработанное организацией, и понимать важность их соблюдения.

Требования законодательства, нормативно-правовых актов и договоров могут налагать ограничения на копирование лицензионных материалов. В частности, они могут требовать, чтобы применялись только те материалы, которые были разработаны в данной организации, либо были переданы на условиях лицензии или предоставлены данной организации разработчиком. Нарушение авторских прав может привести к судебному иску, который повлечет за собой уголовное преследование.

18.1.3 Защита документации организации

Средство управления

Защита документации от утраты, повреждения, фальсификации, несанкционированного доступа и использования несанкционированных версий в соответствии с требованиями законодательства, нормативно-правовых актов, договоров и бизнеса.

Руководство по внедрению

При принятии решения о защите определенной документации организации следует принять во внимание ее классификацию, основанную на системе классификации информации, принятой в организации. Документы должны быть разделены на категории по типам, например, бухгалтерские записи, записи баз данных, журналы регистрации транзакций, журналы аудита и эксплуатационные процедуры; для каждой записи указываются сведения о сроке хранения и типе допущенного к использованию носителя, например, бумага, микрофиша, магнитный или оптический носитель. Все криптографические ключи и программы,

относящиеся к зашифрованным архивам или электронным цифровым подписям (раздел 10), также должны храниться в течение всего срока хранения этих записей, чтобы обеспечить их расшифровку.

Необходимо учитывать возможность ухудшения состояния носителей, используемых для хранения документов. Процедуры хранения и обращения должны быть реализованы в соответствии с требованиями изготовителя.

При выборе электронных средств хранения следует предусмотреть процедуры, обеспечивающие возможность доступа к данным (читаемость носителей и совместимость формата) в течение всего срока хранения, чтобы избежать потери данных по причине изменения в будущем технологии.

Системы хранения данных следует выбирать таким образом, чтобы необходимые данные можно было извлекать за приемлемое время и в нужном формате, в зависимости от требований, подлежащих выполнению.

Система хранения и обработки должна обеспечивать четкую идентификацию записей и периода их хранения в соответствии с требованиями законодательства или нормативно-правовых актов (при наличии). Эта система должна предусматривать адекватное уничтожение записей по истечении периода их хранения, если эти записи больше не нужны организации.

Для достижения целей по защите документации организации следует:

a) разработать руководящие указания по регистрации, хранению, обработке и утилизации записей и информации;

b) составить план-график хранения, определяющий какие записи в течение какого периода времени должны храниться;

c) вести опись источников важной информации.

Дополнительная информация

Согласно требованиям законодательства, нормативно-правовых актов или договоров, а также для поддержания основной бизнес-деятельности организации для некоторых документов может потребоваться обеспечение безопасного хранения. Примерами этому служат документы, которые могут потребоваться в качестве свидетельства того факта, что организация действует в рамках норм, установленных законодательством или нормативно-правовыми актами, для обеспечения защиты от возможного административного или уголовного преследования, либо для подтверждения финансового положения организации по просьбе акционеров, партнеров и аудиторов. Период хранения и содержание подлежащей хранению информации могут быть установлены законодательством или нормативно-правовыми актами.

18.1.4 Обеспечение приватности и защита персональной идентификационной информации

Средство управления

Обеспечение приватности и защиты персональной идентификационной информации, при наличии соответствующих требований в законодательстве и нормативно-правовых актах.

Руководство по внедрению

В организации следует разработать и внедрить политику обработки данных для обеспечения приватности и защиты персональной идентификационной информации. Эта политика должна быть доведена до сведения всех лиц, принимающих участие в обработке персональной идентификационной информации.

Соблюдение этой политики, а также всех соответствующих законов и нормативно-правовых актов, имеющих отношение к обеспечению приватности людей и защите персональной идентификационной информации, требует наличия соответствующей структуры управления и контроля. Часто наилучшим способом добиться этого является назначение ответственного лица, например, специалиста по обеспечению приватности, который должен консультировать руководителей, пользователей и провайдеров услуг по вопросам их персональной ответственности и процедур, требующих соблюдения. Ответственность за обработку персональной идентификационной информации и обеспечение осведомленности относительно принципов обеспечения приватности следует возлагать согласно соответствующему законодательству и нормативно-правовым актам.

Следует внедрить надлежащие технические и организационные меры по защите персональной идентификационной информации.

Дополнительная информация

В ряде стран приняты законы, предусматривающие средства управления сбором, обработкой и передачей персональной идентификационной информации (как правило, информации о существующих людях, которых можно идентифицировать по этой информации). В зависимости от соответствующего законодательства, подобные средства управления могут определять обязанности тех, кто занимается сбором, обработкой и распространением персональной идентификационной информации, а также могут ограничивать передачу персональной идентификационной информации в другие страны.

18.1.5 Регулирование использования криптографических средств защиты информации

Средство управления

Использование криптографических средств защиты информации в соответствии с требованиями всех соответствующих соглашений, законодательства и нормативно-правовых актов.

Руководство по внедрению

Для соблюдения всех соответствующих соглашений, законов и нормативно-правовых актов следует рассмотреть следующие вопросы:

a) ограничения на импорт и/или экспорт аппаратных средств и программного обеспечения, выполняющих криптографические функции;

b) ограничения на импорт и/или экспорт аппаратных средств и программного обеспечения, предназначенных для включения в них криптографических функций;

c) ограничения на использование шифрования;

d) обязательные или дискреционные методы доступа государственных органов к информации, зашифрованной аппаратными или программными средствами для обеспечения конфиденциальности ее содержания.

Чтобы обеспечить соблюдение всех требований соответствующего законодательства и нормативно-правовых актов следует обратиться за консультацией к юристу. Перед передачей зашифрованной информации или криптографических средств защиты информации через границы юрисдикции также необходимо получить консультацию у юриста.

18.2 Аудит и анализ информационной безопасности

Цель: Обеспечить внедрение и функционирование информационной безопасности в соответствии с политиками и процедурами организации.

18.2.1 Независимый аудит информационной безопасности

Средство управления

Независимый аудит подхода организации к управлению информационной безопасностью и ее внедрения (т.е. целей управления, средств управления, политик, процессов и процедур информационной безопасности) через запланированные промежутки времени, или при значительных изменениях в реализации системы обеспечения информационной безопасности.

Руководство по внедрению

Инициатором проведения независимого аудита должно выступать руководство организации. Такого рода независимый аудит необходим для обеспечения постоянного соответствия требованиям, адекватности и эффективности подхода организации к управлению информационной безопасностью. Аудит должен включать оценку возможности улучшения и определение необходимости изменений в подходе к безопасности, включая политику и цели управления.

Такой аудит должен проводиться лицами, которые не зависят от области, подвергаемой аудиту, например, сотрудниками, выполняющими

функции внутреннего аудита, независимым менеджером или сторонней организацией, специализирующейся на проведении аудитов подобного рода. Лица, проводящие подобные аудиты, должны иметь соответствующую квалификацию и опыт.

Результаты независимого аудита должны быть зафиксированы в письменном виде и переданы в качестве отчета руководству организации, инициировавшему ревизию. Следует обеспечить хранение этих отчетов.

Если при проведении независимого аудита выяснится, что принятые в организации подход и внедренное управление информационной безопасностью являются неадекватными, например, если они не соответствуют документированным целям и требованиям или директивам по информационной безопасности, установленным в политиках информационной безопасности (5.1.1), то руководство должно рассмотреть корректирующие меры.

Дополнительная информация

Руководства по проведению независимого аудита содержатся в стандартах O‘z DSt ISO/IEC 27007 и O‘z DSt ISO/IEC TR 27008.

18.2.2 Соответствие политикам и стандартам безопасности

Средство управления

Регулярный анализ соответствия процедур обработки информации соответствующим политикам безопасности, стандартам и любым другим требованиям безопасности, выполняемый руководителями в пределах своей области ответственности.

Руководство по внедрению

При выполнении анализа руководители должны сделать заключение, выполняются ли требования информационной безопасности, определенные в политиках, стандартах и других применяемых нормативно-правовых актах. Регулярный анализ будет более эффективен, если будут учитываться результаты автоматических измерений и отчеты инструментальных средств.

Если в результате выполнения анализа будут обнаружены какие-либо несоответствия, руководителям следует:

a) определить причины несоответствия;

b) оценить потребность в действиях для достижения соответствия;

c) реализовать соответствующие корректирующие действия;

d) выполнить анализ предпринятых корректирующих действий с целью проверки их эффективности и выявления каких-либо недостатков или слабостей.

Результаты выполненного руководителями анализа и корректирующих действий должны быть задокументированы, эти записи необходимо сохранять. Руководители должны сообщать результаты анализа сотрудникам, проводящим независимый аудит (18.2.1), если независимый ревизия проводится в сфере их ответственности.

Дополнительная информация

Оперативный мониторинг использования информационных систем приведен в 12.4.

18.2.3 Анализ соответствия техническим требованиям

Средство управления

Регулярный анализ соответствия информационных систем политикам организации и стандартам в области информационной безопасности.

Руководство по внедрению

Анализ соответствия техническим требованиям предпочтительнее выполнять с помощью автоматизированных инструментальных средств, которые генерируют технические отчеты для последующего анализа техническим специалистом. Этот анализ может выполняться и вручную опытным системным инженером (с использованием подходящих программных инструментальных средств, если это необходимо).

Если используются тесты на проникновение или производится оценка уязвимостей, то необходимо соблюдать осторожность, поскольку подобные действия могут привести к компрометации безопасности системы. Выполнение таких тестов должно быть запланировано, документировано и воспроизводимо.

Любой анализ соответствия техническим требованиям должен выполняться только компетентными, уполномоченными лицами или под их наблюдением.

Дополнительная информация

Анализ соответствия техническим требованиям включает в себя обследование операционных систем для обеспечения того, чтобы аппаратные и программные средства управления были правильно реализованы. Для выполнения анализа соответствия техническим требованиям необходима специализированная техническая экспертиза.

Анализ соответствия техническим требованием также включает в себя, например, тестирование на проникновение и оценку уязвимостей, которые могут выполняться независимыми экспертами, нанятыми специально для этой цели. Это может быть полезно для обнаружения уязвимостей в системе и для проверки того, насколько эффективны средства управления, предотвращающие несанкционированный доступ, возможный из-за этой уязвимости.

Тестирование на проникновение и оценка уязвимостей предусматривают создание моментального снимка системы в определенном состоянии и в определенное время. Моментальный снимок ограничивается теми частями системы, которые в данный момент тестируются в ходе попытки (попыток) проникновения. Тестирование на проникновение и оценка уязвимостей не заменяют определение рисков.

Подробное руководство по проверке соответствия техническим требованиям приведено в O‘z DSt ISO/IEC TR 27008.

Приложение А
(справочное)

Сведения о соответствии ссылочных международных стандартов государственным стандартам Республики Узбекистан

Таблица А.1

Обозначение и наименование ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего государственного стандарта Республики Узбекистан
ISO/IEC 27000:2014 Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь	MOD	O‘z DSt ISO/IEC 27000:2014 Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь
ISO/IEC 27001:2013 Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования	MOD	O‘z DSt ISO/IEC 27001:2016 Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования
ISO/IEC 27005:2011 Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности	MOD	O‘z DSt ISO/IEC 27005:2013 Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности
ISO/IEC 27007:2011 Информационная технология. Методы обеспечения безопасности. Руководящие указания по аудиту систем управления информационной безопасностью	MOD	O‘z DSt ISO/IEC 27007:2015 Информационная технология. Методы обеспечения безопасности. Руководящие указания по аудиту систем управления информационной безопасностью
ISO/IEC TR 27008:2011 Информационная технология. Методы обеспечения безопасности. Руководство для аудиторов по средствам управления информационной безопасностью	MOD	O‘z DSt ISO/IEC TR 27008:2015 Информационная технология. Методы обеспечения безопасности. Руководство для аудиторов по средствам управления, используемых в системах управления информационной безопасностью

Продолжение таблицы А.1

Обозначение и наименование ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего государственного стандарта Республики Узбекистан
ISO/IEC 27031:2011 Информационные технологии. Методы обеспечения защиты. Руководящие указания по готовности информационно-коммуникационных технологий для ведения бизнеса	MOD	O‘z DSt ISO/IEC 27031:2016 Информационная технология. Методы обеспечения безопасности. Руководящие указания по готовности информационно-коммуникационных технологий для ведения бизнеса
ISO/IEC 27033-1:2015 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 1: Обзор и концепции	MOD	O‘z DSt ISO/IEC 27033-1:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 1. Обзор и концепции
ISO/IEC 27033-2:2012 Информационные технологии. Методы и средства обеспечения защиты. Защита сети. Часть 2. Руководящие указания по проектированию и внедрению защиты сети	MOD	O‘z DSt ISO/IEC 27033-2:2016 Информационная технология. Методы обеспечения безопасности. Защита сети. Часть 2 Руководящие указания по проектированию и внедрению защиты сети
ISO/IEC 27033-3:2010 Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления	MOD	O‘z DSt ISO/IEC 27033-3:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления

Окончание таблицы А.1

Обозначение и наименование ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего государственного стандарта Республики Узбекистан
ISO/IEC 27033-4:2014 Информационные технологии. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 4. Коммуникации для обеспечения безопасности между сетями с применением шлюзов безопасности	MOD	O‘z DSt ISO/IEC 27033-4:2016 Информационная технология. Методы обеспечения безопасности Сетевая безопасность. Часть 4. Коммуникации для обеспечения безопасности между сетями с применением шлюзов безопасности
ISO/IEC 27033-5:2013 Информационные технологии. Методы и средства обеспечения безопасности. Безопасность информационной сети. Часть 5. Коммуникации для обеспечения безопасности между сетями с применением виртуальных частных систем	MOD	O‘z DSt ISO/IEC 27033-5:2016 Информационная технология. Методы обеспечения безопасности. Безопасность информационной сети. Часть 5. Коммуникации для обеспечения безопасности между сетями с применением виртуальных частных сетей
ISO/IEC 27035:2011 Информационная технология. Методы обеспечения безопасности. Управление случайностями в системе информационной безопасности	MOD	O‘z DSt ISO/IEC 27035:2015 Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности
Примечание - В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: MOD - модифицированная.		

Приложение В
(справочное)

Технические отклонения и объяснение причин их внесения

В.1 Наименование настоящего стандарта изменено относительно наименования международного стандарта для приведения в соответствие стандартам серии O‘z DSt ISO/IEC 27000.

В.2 По всему тексту слова «международный стандарт» заменены на «настоящий стандарт».

В.3 Стандарт оформлен с учетом требований O‘z DSt 1.6:2003.

В.4 В стандарт включены отдельные изменения и дополнения. Перечень внесенных модификаций и объяснение причин их внесения приведены в таблице В.1.

Таблица В.1 – Перечень внесенных модификаций

Раздел	Модификация	Объяснение
Предисловие	Исключено	В связи с тем, что содержит информацию только о разработке международного стандарта
По всему тексту	Исключены ссылки на международные стандарты	В связи с тем, что указанные ссылки имеют информационно-справочный характер
Раздел 2	Международные стандарты заменены на соответствующие им государственные стандарты	В настоящее время действуют стандарты в соответствии с приложением А
Приложение А	Дополнительно включены в текст стандарта	Приведены сведения о соответствии ссылочных международных стандартов государственным стандартам Республики Узбекистан
Приложение В		Содержит перечень технических отклонений и объяснение причин их внесения

Окончание таблицы В.1

Раздел	Модификация	Объяснение
Библиография	Исключена	Ссылка [1] исключена в связи с исключением предисловия
		Ссылки [2] - [5], [8] - [9], [21] - [27] исключены в связи с исключением ссылок на них в тексте настоящего стандарта
		Ссылки [6] - [7] исключены в связи с отсутствием ссылок на них в тексте международного стандарта
		Ссылки [10] - [20] исключены в связи с тем, что международные стандарты заменены на государственные стандарты в соответствии с приложением А и перенесены в раздел 2

УДК 001.4:025.4:006.354 ОКС 35.040 Т 55

Ключевые слова: доступ, дистанционная работа, информационная безопасность, инцидент, криптографическая защита информации, обмен сообщениями, организация, персонал, политика информационной безопасности, управление, цели и средства управления