МЕЖДУНАРОДНЫЙ СТАНДАРТ

ISO/IEC 27002

Вторая редакция
2013-10-01

Информационные технологии - Методы защиты – Свод рекомендуемых правил для управления информационной безопасностью

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information

Логотип ISO | Логотип IEC

Номер для ссылки
ISO/IEC 27002:2013 (E)

ДОКУМЕНТ С ЗАЩИЩЕННЫМ АВТОРСКИМ ПРАВОМ

Бюро ISO по охране авторских прав
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
Электронная почта copyright@iso.org
Сайт www.iso.org
Издано в Швейцарии

Содержание

Страница

Предисловие

ИСО (Международная организация по стандартизации) и МЭК (Международная электротехническая комиссия) образуют специализированную систему всемирной стандартизации. Государственные органы, являющиеся членами ИСО или МЭК, участвуют в разработке международных стандартов посредством технических комитетов, учрежденных соответствующей организацией для того, чтобы обсуждать определенные области технической деятельности. Технические комитеты ИСО и МЭК сотрудничают в областях взаимного интереса. Другие международные организации, правительственные и неправительственные, контактирующие с ИСО и МЭК, также принимают участие в работе. В области информационных технологий, ИСО и МЭК учредили Совместный технический комитет, ISO/IEC JTC 1.

Проекты международных стандартов составляются в соответствии с правилами, определенными директивами ИСО/МЭК, часть 2.

ISO/IEC 27001 подготовлен Совместным техническим комитетом ISO/IEC JTC 1, Информационные технологии, Подкомитет SC 27, Методы защиты в ИТ.

Обращается внимание на то, что некоторые элементы настоящего международного стандарта могут быть объектом патентных прав. ИСО не несет ответственность за определение какого-либо или всех таких патентных прав.

Данная вторая редакция отменяет и заменяет первую редакцию (ISO/IEC 27002:2005), которая была подвергнута техническому и структурному пересмотру.

0 Введение

0.1 Общие положения и контекст

Настоящий Международный Стандарт был разработан для применения организациями в качестве справочного материала при выборе средств реализации в рамках процесса внедрения системы менеджмента информационной безопасности (СМИБ), основанной на ISO/IEC 27001 [10] или как руководящий документ для организаций, внедряющих широко распространенные средства реализации информационной безопасности. Этот стандарт также предназначен для использования в разрабатываемых руководствах по менеджменту информационной безопасности на предприятиях с отраслевой и организационной спецификой, с учетом создаваемых их окружением рисков для информационной безопасности.

Организации всех типов и размеров (включая государственный и частный сектор, коммерческие и некоммерческие) накапливают, обрабатывают, сохраняют и передают информацию в различных формах, включая электронную, физическую и устную (например, собеседования и презентации).

Ценность информации не только в документированных словах, числах и изображениях: знания, понятия, идеи и бренды – вот примеры нематериальных форм информации. В мире, где все взаимосвязано, информация и соответствующие процессы, системы, сети и персонал, осуществляющий их эксплуатацию, обработку и защиту – все это активы, которые, подобно другим важным деловым активам, представляют ценность для бизнеса организации и, следовательно, нуждаются или требуют защиты от различных угроз.

Активы подвержены как преднамеренным, так и случайным угрозам, при этом связанные с ними процессы, системы, сети и люди имеют присущие им уязвимости. Изменения бизнес-процессов и систем или другие внешние изменения (такие как новые законы и регламенты) могут создать новые риски для информационной безопасности. Поэтому, учитывая множество способов, которыми угрозы, используя уязвимости, могут нанести вред организации, можно утверждать, что риски информационной безопасности всегда присутствуют. Результативная защита информации уменьшает эти риски, страхуя организацию от угроз и уязвимостей и, тем самым, уменьшая воздействие на ее активы.

Информационная безопасность достигается внедрением соответствующего набора средств, включая политики, процессы, процедуры, организационные структуры, а также программного и аппаратного обеспечения соответствующего назначения. Эти средства должны быть разработаны и внедрены, а результаты их работы должны отслеживаться, анализироваться и улучшаться там, где это необходимо, чтобы гарантировать достижение конкретных целей организации, как относящихся к безопасности, так и бизнесу в целом. СМИБ, как это определено в ISO/IEC 27001 [10], дает целостное, согласованное представление о рисках организации в сфере информационной безопасности в целях осуществления всестороннего комплекса мер по обеспечению информационной безопасности в рамках целостной системы менеджмента.

Многие информационные системы были разработаны без учета требований к безопасности в контексте ISO/IEC 27001 [10] и этого стандарта. Безопасность, обеспечиваемая только техническими средствами, носит ограниченный характер и должна быть дополнена

соответствующим менеджментом и процедурами. Определение, какие средства использовать в конкретном случае, требует тщательного планирования и внимания к деталям. Для успешного функционирования СМИБ требуется ее поддержка всеми сотрудниками организации. Это может также потребовать участия акционеров, поставщиков или других внешних сторон. Также могут потребоваться советы привлекаемых извне специалистов.

В более общем смысле результативная защита информации дает уверенность менеджменту и другим заинтересованным лицам в том, что активам организации обеспечена достаточная безопасность и защита от вреда, что выступает как позитивный бизнес-фактор.

0.2 Требования к информационной безопасности

Важно, что организация устанавливает свои требования по безопасности. Есть три основных источника для задания подобного рода требований:

a) оценка рисков для организации с учетом общей бизнес-стратегии и целей организации. Посредством такой оценки рисков выявляются угрозы активам, определяются уязвимости и вероятности их использования, оценивается потенциальное воздействие;

b) законодательные, нормативные и контрактные требования, которые организация, ее торговые партнеры, подрядчики и поставщики услуг должны выполнить, а также социокультурная среда, в которой они действуют;

c) набор принципов, целей и бизнес-требований для управления, обработки, хранения, передачи и архивирования информации, которые организация разработала для обеспечения своей деятельности.

Ресурсы, используемые для осуществления мер, должны соответствовать тому потенциальному ущербу бизнесу, который может возникнуть из-за проблем с безопасностью в отсутствие этих мер. Результаты оценки риска помогут сориентироваться и определить соответствующие управленческие действия и приоритеты для управления рисками информационной безопасности и осуществления мер, выбранных для защиты от этих рисков.

ISO/IEC 27005 [11] содержит руководящие указания по менеджменту рисков информационной безопасности, включая рекомендации по оценке, обработке, принятии и передаче риска, а также по мониторингу и анализу рисков.

0.3 Выбор средств управления

Средства управления могут быть выбраны из предлагаемых этим стандартом или иного набора мер, а также, если необходимо, могут быть разработаны новые средства, чтобы удовлетворить определенные потребности.

Выбор средств управления зависит от организационных решений, основанных на критериях принятия риска, вариантов обработки риска и общего подхода к управлению рисками, применяемого в организации, а также должен учитывать соответствующее национальное и международное законодательство и регламенты. Выбор также зависит от способа взаимодействия средств управления для обеспечения всесторонней защиты.

Некоторые из средств, предлагаемых в этом стандарте, могут применяться как руководящие принципы для менеджмента информационной безопасности, и подходят большинству организаций. Ниже приведены пояснения по средствам управления с рекомендациями по их реализации. Дополнительную информацию о выборе средств и других вариантах обработки рисков можно найти в ISO/IEC 27005. [11]

0.4 Разработка собственных руководящих документов

Настоящий Международный Стандарт может быть взят за отправную точку при разработке

руководящих документов для конкретной организации. Не все средства управления и рекомендации данного свода правил могут быть применимыми. Кроме того, могут потребоваться дополнительные средства управления и руководящие указания, не включенные в этот стандарт. После разработки документов, содержащих дополнительные руководящие указания или средства управления, могло быть полезным включить ссылки на разделы данного стандарта, там, где это применимо, чтобы облегчить проверку соответствия аудиторам и деловым партнерам.

0.5 О жизненном цикле

Информация имеет свой естественный жизненный цикл, начинающийся созданием и получением, проходящий через хранение, обработку, использование и передачу к конечному разрушению. Ценность активов и риски для них могут меняться в течение их времени жизни (например, раскрытие или кража финансовых отчетов компании становятся гораздо менее значимыми после того, как отчеты были официально опубликованы).

Информационные системы также имеют свой жизненный цикл, в ходе которого они задуманы, определены требования к ним, они спроектированы и разработаны, внедрены, применены, поддерживаются в рабочем состоянии и, наконец, исключены из поддержки и утилизированы. Информационная безопасность должна приниматься во внимание на каждой стадии. Разработка новой системы или изменение существующей дают возможность организации обновить или улучшить средства обеспечения безопасности, учитывая случившиеся инциденты, а также текущие и прогнозируемые риски информационной безопасности.

0.6 Родственные стандарты

В то время как данный стандарт содержит рекомендации по широкому кругу средств обеспечения информационной безопасности, которые обычно применяются в самых разных организациях, остальные стандарты семейства ISO/IEC 27000 предлагают дополнительные рекомендации или требования по другим аспектам общего процесса менеджмента информационной безопасности.

См. ISO/IEC 27000 для общего представления как о СМИБ, так и о семействе стандартов. ISO/IEC 27000 содержит глоссарий, дающий определения большинства терминов, используемых в семействе стандартов ISO/IEC 27000, а также описание области применения и целей каждого из стандартов семейства.

Информационные технологии - Методы защиты - Свод рекомендуемых правил для управления информационной безопасностью

1 Область применения

Настоящий Международный Стандарт содержит рекомендации для стандартов по информационной безопасности организаций и способы практического применения менеджмента информационной безопасности, включая выбор, внедрение и осуществление средств управления, учитывающих риски информационной безопасности организации, создаваемые ее окружением.

Настоящий Международный стандарт разработан для применения организациями, которые имеют намерение:

a) выбрать средства управления в рамках процесса внедрения системы менеджмента информационной безопасности, основанной на ISO/IEC 27001; [10]

b) использовать общепринятые средства управления информационной безопасностью;

c) разработать свои собственные руководящие материалы по менеджменту информационной безопасности.

2 Нормативные ссылки

Настоящий документ ссылается (в целом или на какую-то часть) на следующие документы, которые являются обязательными при его применении. Для датированных ссылок применяют только ту версию, которая была упомянута в тексте. Для недатированных ссылок необходимо использовать самое последнее издание документа (включая любые поправки).

ISO/IEC 27000 *Информационные технологии - Методы защиты – Системы менеджмента информационной безопасности – Общий обзор и словарь*

3 Термины и определения

Для целей настоящего документа применяются термины и определения, данные в ISO/IEC 27000.

4 Структура данного стандарта

Настоящий стандарт в 14 разделах содержит описание 114 средств управления, разделенных на 35 основных категорий.

4.1 Разделы

Средства управления, описываемые в каждом разделе, могут относиться к одной или более основной категории.

Порядок следования разделов в настоящем стандарте не отражает их важности. В зависимости от обстоятельств средства управления из одного или всех разделов могут стать важными, следовательно, организация, применяя настоящий стандарт, должна определять подходящие средства управления в соответствии с их значимостью и их использованием в конкретных бизнес-процессах.

4.2 Категории средств реализации

Для каждой основной категорией средств управления указаны:

a) задача управления, т.е. на достижение чего оно направлено;

b) одно или более средств управления, которые могут быть применены для решения указанной задачи.

Описание средств управления структурировано следующим образом.

Метод реализации

Описание конкретного метода реализации, направленного на решение задачи управления.

Рекомендации по применению

Дает более детальную информацию по осуществлению метода реализации и выполнению установленной задачи. Эти рекомендации могут и не быть полностью применимыми или существенными во всех ситуациях и могут не удовлетворять каким-то конкретным требованиям средств управления организации.

Дополнительная информация

Содержит информацию, которую может потребоваться принять во внимание, например, связанную с юридическими вопросами или ссылками на другие стандарты. Если таковой информации для средства управления не имеется, то эта часть описания будет отсутствовать.

5 Политики информационной безопасности

5.1 Ориентация менеджмента на информационную безопасность

Задача: обеспечить ориентацию менеджмента и поддержку информационной безопасности в соответствии с требованиями бизнеса и соответствующими законодательными и нормативными требованиями.

5.1.1 Политики информационной безопасности

Метод реализации

Должен быть разработан, одобрен руководством, опубликован и доведен до персонала и соответствующих внешних сторон комплекс политик информационной безопасности.

Рекомендации по применению

На высшем уровне организация должна сформулировать «политику информационной безопасности», которая одобрена менеджментом и определяет подход организации к управлению достижением целей в области безопасности.

Политики информационной безопасности должны учитывать требования, вытекающие из:

a) бизнес стратегии;

b) законодательства, регламентов и контрактов;

c) существующих и прогнозируемых угроз информационной безопасности.

Политики информационной безопасности должны содержать положения, касающиеся:

a) определения информационной безопасности, целей и принципов для руководства всеми действиями, связанными с информационной безопасностью;

b) назначения общих и конкретных обязанностей по менеджменту информационной безопасности определенным должностям;

c) процессов обработки отклонений и исключений.

На нижнем уровне политика информационной безопасности должна раскрываться в политиках по соответствующим направлениям, которые далее реализуются в средствах управления информационной безопасностью и, как правило, разделяются в соответствии с потребностями определенных целевых групп в организации или по определенным целевым областям.

Как пример, такие целевые области могут включать:

a) контроль доступа (см. раздел 9);

b) классификацию (и обработку) информации (см. раздел 8.2);

c) физическую защиту и защиту от природных факторов (см. раздел 11);

d) целевые области, ориентированные на конечного пользователя, такие как:

   1) надлежащее использование активов (см. раздел 8.1.3);

   2) принцип чистого стола и чистого экрана (см. раздел 11.2.9);

   3) передача информации (см. раздел 13.2.1);

   4) мобильные устройства и удаленная работа (см. раздел 6.2);

   5) ограничения на установку и использование программ (см. раздел 12.6.2);

e) резервное копирование (см. раздел 12.3);

f) передача информации (см. раздел 13.2);

g) защита от вредоносного кода (см. 12.2);

h) управление техническими уязвимостями (см. раздел 12.6.1);

i) криптографические методы (см. раздел 10);

j) безопасность обмена информацией (см. раздел 13);

k) конфиденциальность и защита персональных данных (см. раздел 18.1.4);

l) отношения с поставщиками (см. раздел 15).

Эти политики должны быть доведены до сведения сотрудников и соответствующих внешних сторон в адекватной, доступной и понятной предполагаемому читателю форме, т.е. в духе требований раздела «Осведомленность, образование и обучение в сфере информационной безопасности» (см. 7.2.2)

Дополнительная информация

Необходимость во внутренних политиках различается в разных организациях. Внутренние политики особенно полезны в более крупных и сложных организациях, где те, кто определяет и утверждает ожидаемый уровень управления, отделены от тех, кто осуществляет средства управления, или в ситуациях, когда политика распространяется в организации на многих людей или многие различные функции. Политики информационной безопасности могут быть сведены в общий документ – «политика информационной безопасности» или образовывать комплект отдельных, но связанных документов.

При передаче политик информационной безопасности за пределы организации следует следить за тем, чтобы при этом не была раскрыта конфиденциальная информация.

Некоторые организации используют иные термины для документов, содержащих, политику, например, «стандарт», «положение» или «правила».

5.1.2 Пересмотр политик информационной безопасности

Метод реализации

Политики информационной безопасности для гарантии их постоянной пригодности, соответствия и результативности должны пересматриваться через запланированные интервалы времени или в случае существенных изменений.

Рекомендации по применению

Каждая политика должна быть закреплена за «владельцем», имеющего подтвержденную руководством ответственность за разработку, пересмотр и оценку политик. Пересмотр должен включать оценку возможностей для улучшения политик организации и подхода к управлению информационной безопасностью в ответ на изменения в окружении организации, деловой среде, законодательстве или технической области.

Пересмотр политик информационной безопасности должен производиться с учетом результатов анализа менеджмента.

Результаты пересмотра должны быть утверждены руководством.

6 Организация информационной безопасности

6.1 Внутренняя организация

Задача: Сформировать основные элементы управления для инициирования и контроля внедрения и эксплуатации средств защиты информации в организации

6.1.1 Должностные функции и обязанности, связанные с информационной безопасностью

Метод реализации

Должны быть определены и назначены все обязанности, связанные с информационной безопасностью.

Рекомендации по применению

Назначение обязанностей, связанных с информационной безопасностью, должно проводиться в соответствии с политиками информационной безопасности (см. 5.1.1). Должны быть определены обязанности, связанные с защитой конкретных активов и выполнением конкретных процессов защиты информации. Должны быть определены обязанности для действий по управлению рисками и, в особенности, для принятия остаточных рисков. Эти обязанности должны обеспечиваться поддержкой, если необходимо, в виде более детальных руководств для конкретных участков и устройств обработки информации. Должны быть определены обязанности на местах для защиты активов и выполнения конкретных процессов защиты информации.

Лица, которым определены обязанности, связанные с безопасностью информации, могут делегировать выполнение задач по защите другим лицам.

Но в любом случае они остаются ответственными и должны убеждаться, что любая делегированная задача выполнена надлежащим образом.

Области, за которые отвечают назначенные лица, должны быть определены. В том числе должно быть сделано следующее:

а) выявлены и определены активы и процессы обеспечения информационной безопасности;

b) должно быть назначено ответственное лицо для каждого актива или процесса обеспечения информационной безопасности, должна быть документирована детализированная информация, касающаяся этой ответственности;

c) должны быть определены и документированы уровни полномочий;

d) для обеспечения способности нести ответственность в сфере информационной безопасности назначенные лица должны быть компетентными в этой области и им должна быть обеспечена возможность развития для поддержания своей компетентности на требуемом уровне;

e) должны быть определены и документированы подходы к координации и контролю информационной безопасности в рамках взаимодействия с поставщиками.

Дополнительная информация

Многие организации возлагают на менеджера информационной безопасности общую ответственность за разработку и внедрение средств защиты информации, за обеспечение выбора средств управления.

При этом ответственность за выделение ресурсов и реализацию средств управления будет зачастую оставаться у конкретных руководителей. Одна из общепринятых практик состоит в том, чтобы каждому активу назначать владельца, который потом будет ответственным за ежедневную его защиту.

6.1.2 Разделение обязанностей

Метод реализации

Вступающие в противоречие друг с другом обязанности и области ответственности должны быть разделены для снижения возможности несанкционированного или ненамеренного изменения или неправильного применения активов организации.

Рекомендации по применению

Необходимо следить за тем, чтобы одно и то же лицо не могло иметь доступ, изменять или применять актив без авторизации или опознавания. Инициирование события должно быть отделено от его авторизации. При разработке средств управления должна учитываться возможность сговора.

Для небольших организаций разделение обязанностей может представлять определенные трудности в реализации, тем не менее, сам принцип должен применяться настолько полно, насколько это возможно и практически целесообразно. Там, где есть трудности с разделением обязанностей, должны применяться другие методы реализации, такие как мониторинг действий, аудиты и контроль руководства.

Дополнительная информация

Разделение обязанностей является методом снижения риска случайного или преднамеренного неправильного применения активов организации.

6.1.3 Контакты с полномочными органами

Метод реализации

Должны поддерживаться соответствующие контакты с полномочными органами.

Рекомендации по применению

Организации должны иметь процедуры, которые определяют, когда и через кого будет осуществляться контакт с полномочным органом (например, правоохранительными органами, контролирующими и надзорными органами) и каким образом выявленная информация по инцидентам информационной безопасности должна будет своевременно

передаваться (например, если есть подозрение на возможное нарушение закона).

Дополнительная информация

Организации, подвергшиеся атаке через Интернет, могут иметь необходимость обращения к полномочным органам для принятия мер против источника атаки.

Поддержание таких контактов может быть требованием, обеспечивающим управление инцидентами информационной безопасности (см. раздел 16), или непрерывность бизнеса и процесс планирования действий в чрезвычайной ситуации (см. раздел 17). Контакты с контролирующими органами также полезны с точки зрения раннего информирования и подготовки к предполагаемым изменениям в законодательстве или нормативных требованиях, которые организации должны будут выполнить. Другие полномочные органы, с которыми могут поддерживаться контакты, включают в себя коммунальные и аварийные службы, поставщиков электроэнергии, службы спасения, например, пожарных (в свете непрерывности бизнеса), телекоммуникационных провайдеров (в плане маршрутизации и доступности), а также службы водоснабжения (в плане обеспечения работы охлаждающих устройств для оборудования).

6.1.4 Контакты с профессиональными сообществами

Метод реализации

Должны поддерживаться соответствующие контакты с профессиональными сообществами или иными форумами специалистов по информационной безопасности и профессиональными ассоциациями.

Рекомендации по применению

Членство в профессиональных сообществах или форумах должно рассматриваться как средство для:

a) расширения знаний о лучших практиках и получения самой последней информации в области информационной безопасности;

b) гарантии того, что представление об аспектах информационной безопасности является актуальным и полным;

c) раннего получения предупреждений об опасности, информационных бюллетеней и патчей, касающихся атак и уязвимостей;

d) обеспечения возможности получения советов от специалистов по информационной безопасности;

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

f) обеспечения соответствующих контактов при обработке инцидентов информационной безопасности (см. раздел 16).

Дополнительная информация

Для улучшения сотрудничества и координации в вопросах безопасности могут формироваться соглашения об обмене информацией. Такие соглашения должны определять требования к защите конфиденциальной информации.

6.1.5 Информационная безопасность в управлении проектами

Метод реализации

Вопросы информационной безопасности должны приниматься во внимание в управлении проектами вне зависимости от типа проекта.

Рекомендации по применению

Меры по обеспечению информационной безопасности должны быть интегрированы в методы управления проектами в организации, чтобы гарантировать, что риски информационной безопасности выявлены и обработаны в рамках проекта. Это относится, как правило, к любому проекту вне зависимости от его характера, например, проектам для основного бизнес-процесса, ИТ, обслуживания оборудования и другим поддерживающим процессам. Применяемые методы управления проектами должны предусматривать, что:

a) цели информационной безопасности включены в цели проекта;

b) оценка рисков информационной безопасности проводится на ранней стадии проекта для определения необходимых средств управления;

c) защита информации является частью всех этапов применяемой методологии проекта.

Возможные последствия для информационной безопасности должны учитываться и анализироваться регулярно во всех проектах. Обязанности по информационной безопасности должны быть определены и связаны с конкретными должностями в рамках принятой методологии управления проектом.

6.2 Мобильные устройства и удаленная работа

Задача: гарантировать безопасность при удаленной работе и использовании мобильных устройств

6.2.1 Политика в отношении мобильных устройств

Метод реализации

Должны быть приняты политика и меры по обеспечению безопасности для управления рисками, связанными с использованием мобильных устройств.

Рекомендации по применению

При использовании мобильных устройств особое внимание должно быть уделено гарантии того, что не будет разглашена информация, представляющая коммерческую тайну. Политика в отношении мобильных устройств должна принимать во внимание риски использования мобильных устройств в незащищенных средах.

Политика в отношении мобильных устройств должна предусматривать:

a) регистрацию мобильных устройств;

b) требования по физической защите;

c) ограничения на установку программного обеспечения;

d) требования к версиям программ и применяемым патчам;

e) ограничения на пользование информационными услугами;

f) контроль доступа;

g) криптографические технологии;

h) защиту от вредоносного кода;

i) удаленное выключение, стирание или блокировку;

j) резервное копирование;

k) использование веб-сервисов и веб-приложений.

Необходимо соблюдать осторожность при использовании мобильных устройств в общественных местах, конференц-залах и других незащищенных местах. Должна быть обеспечена защита, чтобы избежать неавторизованного доступа или раскрытия информации, которая хранится или обрабатывается устройствами, например, применением

криптографических методов (см. раздел 10) и принудительным применением секретной информации для аутентификации (см. 9.2.4).

Дополнительная информация

Мобильные устройства для беспроводных соединений похожи на другие типы устройств соединения с сетями, но имеют важные отличия, которые должны быть учтены при определении средств управления. Типичными отличиями являются:

a) некоторые протоколы защиты для беспроводных коммуникаций несовершенны и имеют известные уязвимости;

b) информация, хранимая на мобильных устройствах, не может быть сохранена в виде резервной копии в силу ограниченности пропускной способности сети или же потому, что мобильное устройство не подключено к сети в те моменты времени, когда по расписанию происходит резервное копирование.

Мобильные устройства, как правило, имеют общие функции со стационарно используемыми устройствами, например, работа в сети, доступ к интернету, электронную почту и управление файлами. Средства управления информационной безопасностью для мобильных устройств, обычно, включают в себя те же, что применяются для стационарно используемых устройств, а также те, что нацелены на защиту от угроз, связанных с использованием устройств вне помещений организации.

6.2.2 Удаленная работа

Метод реализации

Должны быть приняты политика и меры обеспечения безопасности для защиты информации, к которой осуществляется доступ на удаленных рабочих местах и которая там обрабатывается или сохраняется.

Рекомендации по применению

Организации, практикующие удаленную работу, должны разработать политику, которая определяет условия и ограничения для дистанционной работы. Там, где это применимо и допустимо с точки зрения закона, может быть принято во внимание следующее:

a) существующий уровень физической защиты удаленного места работы с учетом физической защиты здания и местных условий;

b) предлагаемые физические условия удаленной работы;

c) требования к безопасности коммуникаций, принимая во внимание необходимость удаленного доступа к внутренним системам организации, степень важности информации, к которой будет осуществляться доступ, и которая будет передаваться по каналам связи, а также уязвимость внутренней системы;

d) предоставление виртуального рабочего стола, который предотвращает обработку и сохранение информации на личном оборудовании;

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

f) использование домашних сетей и установление требований или ограничений на конфигурацию сервисов беспроводных сетей;

g) политики и процедуры для предотвращения споров относительно прав на интеллектуальную собственность, созданную на личном оборудовании;

h) препятствия для доступа к личному оборудованию (для проверки его безопасности или в ходе расследования) законодательного характера;

i) лицензионные соглашения на программное обеспечение, в соответствии с которыми организация может нести ответственность за лицензирование клиентского программного обеспечения на личных рабочих станциях сотрудников или внешних пользователей;

j) требования к защите от вредоносного кода и брандмауэрам.

Предполагаемые рекомендации и мероприятия должны включать в себя:

a) обеспечение подходящим оборудованием и устройствами хранения для удаленной работы в тех случаях, когда применение личного оборудования, находящегося вне контроля организации, не разрешено;

b) определение разрешенных работ, графика работ, категорий информации, которую можно обрабатывать, а также внутренних системы и сервисов, к которым работающий удаленно имеет доступ;

c) обеспечение соответствующего коммуникационного оборудования, включая способы удаленного безопасного доступа;

d) физическую защиту;

e) правила и рекомендации по доступу членов семьи и гостей к оборудованию и информации;

f) оказание технической поддержки и обслуживания оборудования и программного обеспечения;

g) страхование;

h) процедуры резервного копирования и обеспечения непрерывности бизнеса;

i) аудит и мониторинг безопасности;

j) прекращение полномочий и прав доступа, а также возврат оборудования при завершении удаленных работ.

Дополнительная информация

Термин «удаленная работа» относится ко всем формам работ вне офиса, включая такие как «telecommuting», «flexible workplace» (гибкое рабочее место), «remote work» и «virtual work» (виртуальное рабочее место)[1].

7 Безопасность персонала

7.1 До приема на работу

Задача: гарантировать, что сотрудники и привлекаемые по контракту понимают свои обязанности и соответствуют тем должностным функциям, которые им предполагается поручить.

7.1.1 Предварительная проверка

Метод реализации

Проверка при приеме на работу, осуществляемая для всех кандидатов, должна проводиться в рамках соответствующих законодательных актов, регламентов и этических норм, а также должна быть соразмерна бизнес-требованиям, категории информации по классификации, к которой предполагается доступ, и предполагаемым рискам.

Рекомендации по применению

Проверка должна проводиться с учетом соответствующей конфиденциальности, защиты

[1] Термины приведены в оригинальной форме на английском языке, т.к. в русском они имеют, практически, один и тот же перевод: удаленная/дистанционная работа [прим. пер.]

персональных данных и трудового законодательства и должна, так где это разрешено, включать следующее:

a) наличие удовлетворительных характеристик, например, одной от организации и одной от конкретного лица,

b) проверка (на полноту и точность) резюме кандидата,

c) подтверждение заявленного образования и профессиональной квалификации,

d) независимая проверка личности (паспорт или иной подобный документ),

e) более детальная проверка, например, кредитной истории или наличие криминального прошлого.

В тех случаях, когда сотрудник принимается на должность, связанную с информационной безопасностью, организация должна убедиться, что кандидат:

a) имеет необходимую компетентность для этой должности,

b) достоин доверия на этой должности, особенно, когда она критически влияет на организацию.

В тех случаях, когда работа, либо поручаемая изначально, либо в результате повышения, требует для исполнителя наличия доступа к средствам обработки информации и, в особенности, если это обработка конфиденциальной информации, например, финансовой, или строго конфиденциальной информации, организация должна также предусмотреть более детальные проверки.

Процедуры должны определять критерии и ограничения для проверок, например, кто имеет право проверять людей и каким образом, когда и почему выполняются проверки.

Процесс проверки также должен проводиться и для тех, кого принимают по контракту. В этом случае должно быть заключено соглашение между организацией и принимаемым по контракту, определяющее ответственность за проведение проверки и процедуры уведомления, которые необходимо выполнить, если проверка не была завершена или ее результаты дают основания для сомнений и беспокойства.

Информация о всех кандидатах, рассматриваемых на позиции в организации, должна собираться и обрабатываться согласно действующему в соответствующей юрисдикции законодательству. В зависимости от действующего законодательства кандидаты должны информироваться заранее о мероприятиях в рамках проверки.

7.1.2 Условия трудового соглашения

Метод реализации

Трудовые соглашения с сотрудниками или привлекаемыми по контракту должны устанавливать их и организации ответственность в части информационной безопасности.

Рекомендации по применению

Контрактные обязательства для сотрудников или работающих по контракту должны отражать политики организации в отношении информационной безопасности дополнительно к разъяснению и установлению:

a) что все сотрудники и работающие по контракту, кто имеет доступ к конфиденциальной информации, должны подписать соглашение о неразглашении конфиденциальной информации до того, как они получат доступ к устройствам обработки информации (см. 13.2.4);

b) юридической ответственности и прав сотрудников и работающих по контракту, например, касающихся законодательства о защите авторских прав или защите данных

(см. 18.1.2 и 18.1.4);

c) обязанностей по классификации информации и управлению ею и другими активами организации, связанными с информацией, устройствами обработки информации и информационными услугами, используемыми сотрудником или работающими по контракту (см. раздел 8);

d) обязанностей сотрудника или работающего по контракту по обработке информации, полученной от других компаний или внешних сторон;

e) действий, которые должны быть предприняты, если сотрудник или работающий по контракту игнорирует требования организации по безопасности (см. 7.2.3).

Функции и обязанности в отношении информационной безопасности должны быть доведены до сведения кандидатов на должность в процессе, предшествующем приему на работу.

Организация должна гарантировать, что сотрудники и работающие по контракту согласны с положениями и условиями, относящимися к информационной безопасности, соответствующими характеру и уровню доступа, который они будут иметь к активам организации, связанным с информационными системами и сервисами.

Там, где это возможно, обязанности, установленные положениями и условиями найма, должны быть продлены на определенный период и после прекращения трудовых отношений (см. 7.3).

Дополнительная информация

Для установления обязанностей сотрудника или работающего по контракту в отношении информационной безопасности, касающихся конфиденциальности, защиты данных, правил поведения, надлежащего использования оборудования организации, а также ожидаемого организацией следования признанным практикам, может быть использован Кодекс поведения. Внешняя сторона, с которой связан работающий по контракту, может быть обязана вступать в договорные отношения от имени контрактора.

7.2 В период занятости

Задача: гарантировать, что сотрудники и работающие по контракту знают и выполняют свои обязанности, связанные с информационной безопасностью.

7.2.1 Ответственность руководства

Метод реализации

Руководство должно требовать от всех сотрудников и работающих по контракту соблюдения требований по информационной безопасности в соответствии с установленными политиками и процедурами организации.

Рекомендации по применению

Ответственность руководства должна включать в себя гарантию того, что сотрудники и работающие по контракту:

a) должным образом проинформированы о своей роли и ответственности, связанными с информационной безопасностью, до того, как получили доступ к конфиденциальной информации и информационным системам;

b) обеспечены руководящими указаниями, устанавливающими те ожидания в отношении информационной безопасности, которые связаны с их ролью в организации;

c) мотивированы на выполнение политик информационной безопасности организации;

d) осведомлены в вопросах информационной безопасности на том уровне, который

соответствует их роли и ответственности в организации;

e) согласны с условиями занятости, которые включают политику информационной безопасности организации и соответствующие методы работы;

f) сохраняют соответствующий уровень навыков и квалификацию, а также проходят обучение на регулярной основе;

g) имеют канал для анонимного информирования о нарушениях политик или процедур информационной безопасности («информирование о нарушениях»).

Руководство должно демонстрировать поддержку политик, процедур и средств управления информационной безопасностью, а также действовать соответственно своей роли.

Дополнительная информация

Если сотрудники и работающие по контракту не были осведомлены об их ответственности в сфере информационной безопасности, это может нанести заметный урон организации. Мотивированный персонал будет, вероятно, более надежным и вызывать меньше инцидентов информационной безопасности.

Плохое управление может привести к тому, что персонал будет чувствовать себя недооцененным, что может выразиться в негативном влиянии на информационную безопасность организации. Например, плохое управление может приводить к пренебрежению информационной безопасностью или возможному неправильному применению активов организации.

7.2.2 Осведомленность, образование и обучение в сфере информационной безопасности

Метод реализации

Все сотрудники организации и, там, где это существенно, работающие по контракту должны быть соответствующим образом информированы и обучены, а также регулярно извещаться об изменениях в политиках и процедурах организации, в той мере, насколько это важно для исполнения их служебных обязанностей.

Рекомендации по применению

Программа по информированию в области информационной безопасности должна быть нацелена на донесение до сотрудников и, там, где это существенно, работающих по контракту их обязанностей в области информационной безопасности и средств, которыми эти обязанности могут быть исполнены.

Программа по информированию в области информационной безопасности должна быть согласована с политиками и соответствующими процедурами информационной безопасности организации, а также принимать во внимание информацию, которая должна быть защищена, и меры, которые были предприняты для ее защиты. Программа должна включать в себя ряд информационно-агитационных мероприятий, например, таких как «день информационной безопасности», выпуск брошюр или информационных листков.

Программа по информированию должна планироваться с учетом той роли, которую играют сотрудники в организации, и, там, где это существенно, ожиданий организации от осведомленности работающих по контракту. Мероприятия программы должны быть рассчитаны на продолжительный период, желательно быть регулярными с тем, чтобы они повторялись и охватывали новых сотрудников и работающих по контракту. Программа также должна регулярно обновляться с тем, чтобы постоянно соответствовать политикам и процедурам организации, а также использовать уроки, извлеченные из инцидентов информационной безопасности.

Вводный курс должен проводиться так, как это предусмотрено программой по информированию в области информационной безопасности организации. Для вводного курса могут использоваться различные методы обучения, включая занятие в классах, дистанционное обучение, обучение онлайн, самостоятельные занятия и другие.

Обеспечение осведомленности и подготовка в области информационной безопасности должны также раскрывать такие общие вопросы, как:

a) приверженность руководства информационной безопасности;

b) необходимость в ознакомлении и выполнении правил и обязанностей, связанных с информационной безопасностью, как это определено в политиках, стандартах, законах, регламентах, контрактах и соглашениях;

c) персональная ответственность за действие или бездействие, а также общая ответственность относительно безопасности или защиты информации, принадлежащей организации или внешним сторонам;

d) основные процедуры информационной безопасности (такие, как отчеты по инцидентам информационной безопасности) и основные средства реализации (такие, как безопасные пароли, контроль вредоносных программ и политика чистого стола);

e) контакты и ресурсы для получения дополнительной информации и рекомендаций по вопросам информационной безопасности, включая дополнительные материалы для обучения и подготовки в области информационной безопасности.

Обучение и подготовка в области информационной безопасности должны проводиться периодически. Начальное обучение и подготовка проводятся для тех, кто переходит на новую позицию или получает обязанности с существенно отличающимися требованиями к информационной безопасности, а не только к тем, кто только начинает работу, при этом обучение должно проводиться до того, как сотрудник приступит к исполнению обязанностей.

Организация должна разработать программу обучения и подготовки для того, чтобы они проводились результативно. Программа должна быть согласована с политиками и соответствующими процедурами информационной безопасности организации, а также принимать во внимание информацию, которая должна быть защищена, и меры, которые были предприняты для ее защиты. Программа должна предусматривать различные формы обучения и подготовки, например, лекции или самообучение.

Дополнительная информация

При формировании программы важно фокусировать внимание не только на «что» и «как», но и «почему». Важно, чтобы сотрудники понимали цели информационной безопасности и возможное влияние – позитивное или негативное – которое оказывают на организацию их действия.

Информирование, обучение и подготовка могут быть частью других обучающих мероприятий, или выполняться совместно с ними, например, общими тренингами по ИТ или безопасности. Мероприятия по информированию, обучению и подготовке должны соответствовать конкретным обязанностям, ответственности и навыкам.

В конце курса может проводиться оценка усвоения сотрудником материала.

7.2.3 Дисциплинарные меры

Метод реализации

Должен быть разработан и доведен до сведения персонала процесс для принятия мер к тем сотрудникам, которые допустили нарушение требований информационной безопасности.

Рекомендации по применению

Дисциплинарные меры не могут быть применены без предварительной проверки того, что нарушение информационной безопасности действительно имело место (см. 16.1.7).

Установленные дисциплинарные меры должны гарантировать корректность и справедливость в отношении сотрудников, которые подозреваются в нарушении информационной безопасности. Установленные дисциплинарные меры должны приниматься как соответствующий ответ, который учитывает такие факторы, как характер и серьезность нарушения и его влияние на бизнес, допущено ли оно в первый раз или повторно, был ли нарушитель надлежащим образом обучен, имеющееся соответствующее законодательство, бизнес-контракты и другие необходимые факторы.

Дисциплинарные меры должны также применяться как профилактическое средство для предотвращения нарушений сотрудниками политики и процедур информационной безопасности организации и иных нарушений в этой области. Намеренно совершаемые нарушения могут потребовать немедленных действий.

Дополнительная информация

Дисциплинарные меры могут также быть мотивирующим или стимулирующим фактором, если предусматриваются поощрительные меры в случае образцового поведения в части информационной безопасности.

7.3 Прекращение и изменение трудовых отношений

Задача: защитить интересы организации при изменении обязанностей сотрудника или прекращении с ним трудовых отношений

7.3.1 Освобождение от обязанностей или их изменение

Метод реализации

Должны быть определены, доведены до сведения сотрудника или работающего по контракту его область ответственности и обеспечено выполнение его обязанностей в отношении информационной безопасности, остающихся в силе после прекращения или изменения трудовых отношений.

Рекомендации по применению

Предупреждение о прекращении трудовых отношений должно включать в себя информацию о существующих требованиях в сфере информационной безопасности и юридических обязательствах, а также, там, где это применимо, обязательствах, вытекающих из соглашения о конфиденциальности (см. 13.2.4) и условиях трудоустройства (см. 7.1.2), сохраняющих свою силу в течение определенного периода после завершения трудовых отношений с сотрудником или работающим по контракту.

Ответственность и обязанности, которые остаются в силе после завершения трудовых отношений, должны быть указаны в условиях трудового соглашения с сотрудником или контракте (см. 7.1.2).

Изменения в должностных функциях или обязанностях должны управляться так же, как и в случае прекращения трудовых отношений, но дополненные возложением новых обязанностей и должностных функций.

Дополнительная информация

Подразделение по управлению персоналом несет общую ответственность за процесс прекращения трудовых отношений и взаимодействует с руководителем увольняющегося сотрудника в части выполнения соответствующих процедур, относящихся к

информационной безопасности. Если речь идет о работающем по контракту представителе внешней стороны, то процесс завершения трудовых отношений ведется внешней стороной в соответствии с контрактом между ею и организацией.

Возможно, потребуется информировать персонал, потребителей или подрядчиков об изменениях в штате и организационной структуре.

8 Управление активами

8.1 Ответственность за активы

Задача: выявить активы организации и определить соответствующую ответственность по их защите

8.1.1 Инвентаризация активов

Метод реализации

Информация, другие активы, связанные с информацией и устройствами обработки информации, должны быть выявлены и составлен реестр этих активов, который должен поддерживаться в актуальном состоянии.

Рекомендации по применению

Организация должна выявить активы, поддерживающие жизненный цикл информации, и документально зафиксировать их значимость. Жизненный цикл информации должен включать в себя создание, обработку, хранение, передачу, стирание и уничтожение. Документация соответствующим образом должна быть зафиксирована в специально созданных или уже существующих реестрах.

Реестр активов должен быть точным, актуальным, полным и соответствующим другим реестрам.

Для каждого выявленного актива должен быть назначен владелец (см. 8.1.2) и проведена классификация (см. 8.2).

Дополнительная информация

Реестры активов способствуют обеспечению результативной защиты и могут быть также востребованы для других целей, таких как охрана здоровья и труда, страхование или финансы (менеджмент активов).

Стандарт ISO/IEC 27005 [11] дает примеры активов, которые могут быть приняты во внимание организацией в ходе выявления активов. Процесс составления реестра активов является важной предпосылкой управления рисками (см. также ISO/IEC 27000 и ISO/IEC 27005 [11]).

8.1.2 Владение активами

Метод реализации

У активов, включенных в реестр, должны быть владельцы.

Рекомендации по применению

Отдельные лица, равно как и подразделения, имеющие утвержденную ответственность за актив в течение его жизненного цикла, могут быть назначены владельцами актива.

Процесс, гарантирующий своевременное назначение владельца актива, как правило, выполняется. Владелец должен быть назначен, когда актив создается или когда передается в организацию. Владелец актива должен нести ответственность за надлежащее управление

активом на протяжении всего жизненного цикла актива.

Владелец актива должен:

a) гарантировать, что активы включены в реестр;

b) гарантировать, что активы надлежащим образом классифицированы и защищены;

c) установить и периодически пересматривать ограничения доступа и классификацию важных активов, принимая во внимание действующие политики контроля доступа;

d) гарантировать надлежащие действия с активом, когда он удаляется или уничтожается.

Дополнительная информация

Назначенный владелец может быть либо отдельным лицом, либо подразделением, которое имеет утвержденную ответственность за актив на протяжении всего его жизненного цикла. Назначение владельцем процесса не дает прав собственности на актив.

Выполнение типовых задач может быть делегировано, например, ответственному за хранение, который следит за активом на ежедневной основе, но при этом ответственность остается на владельце.

В сложных информационных системах может быть полезно определять группу активов, которые совместно обеспечивают определенный сервис. В этом случае владелец этого сервиса является ответственным за поставку этого сервиса, включая действия с его активами.

8.1.3 Надлежащее использование активов

Метод реализации

Правила для надлежащего использования информации и активов, связанных с информацией и устройствами обработки информации, должны быть определены, документированы и внедрены.

Рекомендации по применению

Сотрудники и внешние пользователи, использующие или имеющие доступ к активам организации, должны быть осведомлены о требованиях информационной безопасности, относящихся к информации и другим активам организации, которые связаны с информацией, устройствами и ресурсами для обработки информации. Они должны нести ответственность за применение ими любых ресурсов обработки информации и любое подобное использование, осуществляемое в зоне их ответственности.

8.1.4 Возврат активов

Метод реализации

Все сотрудники и внешние пользователи должны вернуть все активы организации в ее распоряжение по окончании действия трудовых договоров, контрактов и соглашений.

Рекомендации по применению

Процесс прекращения трудовых отношений должен быть установлен так, чтобы включать в себя возврат всех ранее выданных физических или электронных активов, принадлежащих или доверенных организации.

В тех случаях, когда сотрудник или внешний пользователь купил оборудование организации или использует свое личное оборудование, процедуры должны быть такими, чтобы гарантировать, что соответствующая информация передана в организацию и надежным способом стерта с этого оборудования (см. 11.2.7).

В тех случаях, когда сотрудник или внешний пользователь обладает знаниями, ценными для

текущей деятельности, такого рода информация должна быть документирована и передана в организацию.

В период времени после уведомления до прекращения трудовых отношений организация должна контролировать неавторизованное копирование соответствующей информации (например, интеллектуальной собственности) со стороны тех, с кем прекращаются трудовые отношения.

8.2 Классификация информации

Задача: гарантировать, что информация имеет уровень защиты, соответствующий ее значимости для организации

8.2.1 Классификация информации

Метод реализации

Информация должна быть классифицирована с точки зрения юридических требований, содержания, критичности и уязвимости для несанкционированного раскрытия и изменения.

Рекомендации по применению

Классификация и связанные с нею методы защиты информации должны учитывать потребности бизнеса в обмене информацией или ограничения доступа к ней, равно как и законодательные требования. Активы, отличающиеся от информации, могут также быть классифицированы в соответствии с классификацией для информации, которая в них хранится, обрабатывается или иным образом преобразуется, или защищается этими активами.

Владельцы активов должны быть ответственными за их классификацию.

Схема классификации должна включать в себя соглашение о классификации и критерии для пересмотра классификации через какое-то время. Уровень защиты в схеме должен быть оценен на основе анализа конфиденциальности, целостности и возможности применения, а также любых других требований, связанных с информацией. Схема должна быть согласована с политикой контроля доступа (см. 9.1.1).

Каждому уровню должно быть присвоено наименование, которое имеет смысл в контексте применения этой классификационной схемы.

Схема должна быть единой для всей организации, чтобы все, кто будут классифицировать информацию и связанные с ней активы, делали это одинаково, имели общее понимание требований защиты и применяли соответствующие меры защиты.

Классификация должна быть включена в процессы организации, быть единой и логически непротиворечивой в рамках организации. Результаты классификации должны отражать ценность активов, зависящую от их степени закрытости и значимости для организации, например, с точки зрения конфиденциальности, целостности и возможности применения. Результаты классификации должны обновляться в соответствии с измерениями этой ценности, степени конфиденциальности и значимости в течение всего их жизненного цикла.

Дополнительная информация

Классификация дает тем, кто работает с информацией, четкое понимание, как обращаться с ней и защищать ее. Формирование категорий информации по одинаковым необходимым мерам защиты и определение процедур информационной безопасности, которые применяются ко всей информации каждой категории, облегчает эту задачу. Такой подход снижает потребность в оценке рисков и выборе средств реализации в каждом отдельном случае.

Степень конфиденциальности или значимости информации может меняться по истечении определенного периода времени, например, после ее опубликования. Подобные факторы должны приниматься во внимание, т.к. отнесение к более высокой категории может вести к применению методов реализации, в которых нет необходимости, что ведет к дополнительным расходам, или наоборот, отнесение к более низкой категории может ставить под угрозу достижение бизнес-целей.

Примерная схема классификации по конфиденциальности, может основываться на следующих четырех уровнях:

a) раскрытие не вызывает ущерба;

b) раскрытие создает некоторые затруднения или небольшие проблемы в операционной деятельности;

c) раскрытие оказывает существенный кратковременный эффект на операционную деятельность или достижение тактических целей;

d) раскрытие оказывает серьезное влияние на достижение долговременных стратегических целей или подвергает риску само существование организации.

8.2.2 Маркировка информации

Метод реализации

Должен быть разработан и внедрен соответствующий набор процедур для маркировки информации в соответствии со схемой классификации информации, принятой в организации.

Рекомендации по применению

Процедуры для маркировки информации должны охватывать информацию и связанные с ней активы, как в физической, так и в электронной форме. Маркировка должна соответствовать схеме классификации, установленной в п. 8.2.1. Маркировка должна легко распознаваться. Процедуры должны содержать руководящие указания, где и как размещается маркировка с учетом того, каким образом осуществляется доступ к информации или способов использования активов, зависящих от типа носителя. Процедуры должны определять ситуации, когда маркировка – во избежание лишних затрат – не требуется, например, для информации, не являющейся конфиденциальной. Сотрудники и работающие по контракту должны быть ознакомлены с процедурами маркировки информации.

Результаты, формируемые системами, содержащим информацию, которая классифицирована как конфиденциальная или значимая, должны обрабатываться соответственно классификационной категории.

Дополнительная информация

Маркировка конфиденциальной информации является ключевым требованием для мероприятий по обмену информацией. Обычной формой маркировки является наклеивание этикеток и указание метаданных.

8.2.3 Обращение с активами

Метод реализации

Должны быть разработаны и внедрены процедуры обращения с активами в соответствии со схемой классификации информации, принятой в организации.

Рекомендации по применению

Процедуры должны быть разработаны для обращения, обработки, хранения и передачи

информации в соответствии с категорией классификации (см. 8.2.1).

Должны приниматься во внимание следующие факторы:

a) ограничения доступа, обеспечивающие выполнение требований по защите для каждой категории классификации;

b) ведение документированного реестра уполномоченных обладателей активов;

c) защита временных или постоянных копий информации на уровне, соответствующем защите оригинальной информации;

d) хранение ИТ-активов в соответствии с указаниями производителей;

e) четкая маркировка всех копий носителей для информирования уполномоченного обладателя.

Схема классификации, используемая в организации, может не совпадать с подобными схемами в других организациях, даже если совпадают наименования категорий; к тому же, информация, передаваемая между организациями, может относиться к разным категориям классификации в зависимости от ситуации в каждой организации, даже если их схемы классификации идентичны.

Соглашения с другими организациями, которые предполагают совместное использование информации, должны включать в себя процедуры определения классификации такой информации и интерпретации категорий классификации для других организаций.

8.3 Обращение с носителями информации

Задача: предотвратить несанкционированное раскрытие, изменение, перемещение или уничтожение информации, хранимой на носителе.

8.3.1 Управление съемными носителями информации

Метод реализации

Должны быть внедрены процедуры для управления съемными носителями в соответствии со схемой классификации, принятой в организации.

Рекомендации по применению

Для управления съемными носителями должны быть учтены следующие рекомендации:

a) содержимое, в котором отпала необходимость, на любых многократно используемых носителях, которые могут быть вынесены из организации, должна быть удалена без возможности восстановления,

b) там, где это необходимо и целесообразно, должно требоваться разрешение для носителей, выносимых с территории организации, и записи о выносе должны сохраняться для предъявления в качестве свидетельств при аудите,

c) все носители должны храниться в безопасном, защищенном месте в соответствии с требованиями производителя,

d) в том случае, если данные являются конфиденциальными или важна их целостность, должны применяться криптографические методы для защиты данных на съемных носителях,

e) для снижения риска, связанного с ухудшением свойств носителя от времени, в том случае, когда данные еще необходимы, они должны быть переписаны на свежий носитель до того, как станут нечитаемыми,

f) несколько копий важных данных должны сохраняться на отдельных носителях для снижения риска одновременной потери или повреждения данных,

g) должна предусматриваться регистрация съемных носителей для ограничения возможности потери данных,

h) съемные носители должны применяться только в том случае, если это оправдано потребностями бизнеса,

i) там, где есть необходимость применения съемных носителей, перенос информации на них должен контролироваться.

Процедуры и уровни авторизации должны быть документированы.

8.3.2 Утилизация носителей информации

Метод реализации

Носители, если в них больше нет необходимости, должны быть утилизированы надежным способом в соответствии с установленными процедурами.

Рекомендации по применению

Должны быть установлены формальные процедуры для надежной утилизации носителей с целью минимизации риска утечки конфиденциальной информации к лицам, которым она не предназначена. Процедуры для надежной утилизации носителей, содержащих конфиденциальную информацию, должны соответствовать степени критичности этой информации. При этом должно быть учтено следующее:

a) носители с конфиденциальной информацией должны храниться и утилизироваться надежным способом, например, сжиганием или измельчением, или очищаться от данных для применения другим приложением в организации,

b) процедуры должны быть введены в действие, чтобы определять те элементы, которые могут требовать утилизации,

c) может быть проще организовать для всех носителей сбор и надежную утилизацию, нежели пытаться отделить критичные,

d) многие организации предлагают услуги сбора и утилизации носителей; необходимо внимательно выбирать подходящего внешнего исполнителя, который применяет соответствующие средства и имеет опыт,

e) утилизация критичных носителей должна регистрироваться для предъявления в качестве свидетельства на аудитах.

При накоплении носителей для утилизации следует иметь в виду эффект критической массы, который проявляется в том, что большой массив некритичной информации сам может стать критичным.

Дополнительная информация

Для поврежденных устройств, содержащих конфиденциальные данные, может потребоваться оценка рисков на предмет того, должны ли эти устройства быть физически уничтожены вместо того, чтобы быть отправлены на ремонт или выброшены (см. 11.2.7).

8.3.3 Физическое перемещение носителей информации

Метод реализации

Носители информации во время транспортировки должны быть защищены от несанкционированного доступа, нецелевого использования или повреждения.

Рекомендации по применению

Для защиты транспортируемых носителей, содержащих информацию, должны быть приняты во внимание следующие рекомендации:

a) должен использоваться надежный транспорт или курьеры,

b) перечень авторизованных курьеров должен быть согласован с руководством,

c) должны быть разработаны процедуры для идентификации курьеров,

d) упаковка должна обеспечивать защиту содержимого от любых физических повреждений, которые могут возникнуть в ходе транспортировки, и соответствовать требованиям производителей, например, защита от любых внешних факторов, которые могут снизить возможность восстановления носителей, такие как воздействие тепла, влаги или электромагнитных полей,

e) должны вестись записи, указывающие содержание носителей, примененную защиту, а также время передачи для транспортировки и приема в месте назначения.

Дополнительная информация

Информация может быть уязвимой для несанкционированного доступа, нецелевого применения или повреждения во время физической транспортировки, например, при отправке носителя по почте или через курьера. В этом случае носители включают в себя и бумажные документы.

В тех случаях, когда конфиденциальная информация не зашифрована, должны предусматриваться дополнительные меры физической защиты носителя.

9 Контроль доступа

9.1 Диктуемые бизнесом требования к контролю доступа

Задача: ограничить доступ к информации и устройствам ее обработки.

9.1.1 Политика контроля доступа

Метод реализации

Политика контроля доступа должна быть сформулирована, документирована и пересматриваться с точки зрения требований бизнеса и информационной безопасности.

Рекомендации по применению

Владельцы активов должны определить соответствующие правила для контроля доступа, права доступа и ограничения для определенных категорий пользователей по отношению к их активам с уровнем детализации и строгости контроля, отражающей риски, связанные с информационной безопасностью.

Средства контроля доступа могут быть как логическими, так и физическими (см. раздел 11) и они должны рассматриваться совместно. Пользователям и поставщикам сервисов должны быть ясным образом доведены требования бизнеса, которым должны удовлетворять средства контроля доступа.

Политика должна учитывать следующее:

a) требования по безопасности бизнес-приложений;

b) политики распространения и авторизации информации, например, принцип «знает тот, кому положено знать», уровни информационной безопасности и классификация информации (см. 8.2);

c) соответствие между правами доступа и политиками классификации информации для систем и сетей;

d) соответствующие законодательные и любые контрактные обязательства, касающиеся ограничения доступа к данным или сервисам (см. 18.1);

e) управление правами доступа в распределенных средах и сетях, которые допускают все типы соединений;

f) разделение задач по контролю доступа, например, запрос доступа, авторизация доступа, администрирование доступа;

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

h) требования к периодическому пересмотру прав доступа (см. 9.2.5);

i) отмену прав доступа (см. 9.2.6);

j) архивирование записей всех значимых событий, касающихся использования и управления идентификационной информацией пользователей и секретной информацией для аутентификации;

k) задачи с привилегированным доступом (см. 9.2.3).

Дополнительная информация

Следует проявлять осторожность при формулировании правил контроля доступа, учитывая:

a) установление правил, следующих более принципу «Запрещено все, что не разрешено», нежели «Разрешено все, что не запрещено»;

b) изменения маркировки информации (см. 8.2.2), которые инициируются автоматически устройствами обработки информации и которые инициированы решением пользователя;

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

d) правила, которые требуют определенной процедуры утверждения до вступления в силу, и те, которые этого не требуют;

Правила контроля доступа должны быть зафиксированы в формальных процедурах (см. 9.2, 9.3, 9.4) и под них определены обязанности (см. 6.1.1, 9.3).

Контроль доступа на основе ролей является подходом, который успешно используется многими организациями для связи прав доступа и бизнес-ролей.

Есть два часто применяемых принципа, определяющих политику контроля доступа:

a) «знает тот, кому положено знать»: вы получаете доступ только к той информации, которая необходима для выполнения служебных заданий (различные задания/роли подразумевают различную необходимость и, следовательно, различный профиль доступа);

b) «доступ по потребности»: вы получаете доступ только к тем устройствам обработки информации (ИТ-оборудование, приложения, процедуры, помещения), которые необходимы вам для выполнения задачи/работы/роли.

9.1.2 Доступ к сетям и сетевым службам

Метод реализации

Пользователи должны получать доступ только к тем сетям и сетевым службам, для которых у них есть авторизация.

Рекомендации по применению

Должна быть сформулирована политика, относящаяся к использованию сетей и сетевых служб. Эта политика должна охватывать:

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

b) процедуры авторизации для определения, кому к какой сети или службе разрешен доступ;

c) средства управления и процедуры для защиты доступа к сетевым соединениям и сетевым

службам;

d) средства для доступа к сетям и сетевым службам (например, использование VPN или беспроводной сети);

e) требования к авторизации пользователя для доступа к различным сетевым службам;

f) мониторинг использования сетевых служб.

Политика использования сетевых служб должна быть согласованной с политикой контроля доступа организации (см. 9.1.1).

Дополнительная информация

Несанкционированное или незащищенное подключение к сетевым службам может оказывать влияние на всю организацию. Контроль этого особенно важен для сетевых соединений приложений, критически важных с точки зрения бизнеса, или для пользователей, находящихся в местах с высоким уровнем риска, например, общественных местах или точках за пределами организации, которые вне контроля системы управления информационной безопасностью организации.

9.2 Управление доступом пользователей

Задача: гарантировать авторизованный доступ пользователя и предотвратить несанкционированный доступ к системам и службам.

9.2.1 Регистрация и отмена регистрации пользователя

Метод реализации

Должен быть внедрен формализованный процесс регистрации и отмены регистрации пользователей, обеспечивающий возможность назначения прав доступа.

Рекомендации по применению

Процесс управления идентификаторами пользователей должен включать в себя:

a) использование уникального идентификатора пользователя, позволяющий связать пользователей с их действиями и нести за них ответственность; использование коллективных идентификаторов должно быть разрешено только в тех случаях, когда это необходимо для бизнеса или в силу операционных причин и должно быть утверждено и документировано;

b) немедленная блокировка или удаление идентификатора пользователя, если он покинул организацию (см. 9.2.6);

c) периодическое выявление и удаление или блокировка неактуальных идентификаторов;

d) гарантию того, что неактуальные идентификаторы не выдаются другим пользователям.

Дополнительная информация

Обеспечение или отмена доступа к информации или устройствам обработки информации обычно представляет собой двухшаговую процедуру:

a) назначение и активация или отмена идентификатора пользователя;

b) назначение или отмена прав доступа для этого идентификатора пользователя (см. 9.2.2).

9.2.2 Предоставление доступа пользователю

Метод реализации

Должен быть внедрен формализованный процесс предоставления доступа пользователям для назначения или отмены прав всем типам пользователей ко всем системам и службам.

Рекомендации по применению

Процесс, обеспечивающий назначение или отмену прав, связанных с идентификаторами пользователя, должен включать:

a) получение разрешения от владельца информационной системы или службы на использование этой информационной системы или службы (см. 8.2.2); так же может быть целесообразным отделение подтверждения прав доступа от управления;

b) проверку того, что предоставляемый уровень доступа соответствует политикам доступа (см. 9.1) и согласуется с другими требованиями, такими, как разделение обязанностей (см. 6.1.2);

c) гарантию того, что права доступа не будут активированы (например, поставщиками услуг) до завершения процедур авторизации;

d) ведение централизованной регистрации прав доступа, связываемых с идентификатором пользователя, к информационным системам и службам;

e) изменение прав доступа пользователям, у которых поменялись роли или задачи, а также немедленную отмену или блокирование прав доступа пользователям, ушедшим из организации;

f) периодический пересмотр прав доступа с владельцами информационных систем и служб (см. 9.2.5).

Дополнительная информация

Следует рассмотреть вопрос о введении определяющих права доступа ролей, вытекающих из требований бизнеса, которые объединяют различные права доступа в типовые профили доступа пользователей. Запросы на доступ и их анализ (см. 9.2.4) легче обрабатываются на уровне таких ролей, нежели на уровне отдельных прав.

Следует рассмотреть вопрос включения в контракт сотрудника и контракт на оказание услуг разделов, определяющих санкции в случае попытки неавторизованного доступа, совершаемой сотрудником или работающим по контракту (см 7.1.2, 7.2.3, 13.2.4, 15.1.2).

9.2.3 Управление привилегированными правами доступа

Метод реализации

Назначение и применение привилегированных прав должно быть ограниченным и контролируемым.

Рекомендации по применению

Распределение привилегированных прав доступа должно контролироваться через формализованный процесс авторизации в соответствии с действующей политикой контроля доступа (см 9.1.1). Должны быть предусмотрены следующие шаги:

a) привилегированные права доступа, связанные с каждой системой или процессом, например, операционной системой, системой управления базой данных и каждым приложением, а также пользователями, которым требуется назначение таких прав, должны быть определены;

b) привилегированные права доступа должны быть назначены пользователям по принципу «доступ по потребности» и «доступ по событию» в соответствии с политикой контроля доступа (см 9.1.1), т.е. по минимуму, исходя из их функциональных задач;

c) процесс авторизации и регистрация всех назначенных привилегий должны поддерживаться в управляемой состоянии. Привилегированные права доступа не должны присваиваться до завершения процесса авторизации;

d) должны быть определены требования для установления срока действия привилегированных прав доступа;

e) привилегированные права доступа должны быть связаны с идентификатором пользователя, отличным от того, что используется для исполнения повседневных должностных обязанностей. Эти обязанности не должны выполняться под привилегированным идентификатором;

f) полномочия пользователей с привилегированными правами доступа должны регулярно пересматриваться с целью убедиться, что они соответствуют их обязанностям;

g) должны быть разработаны и поддерживаться конкретные процедуры для избежания неавторизованного использования общих администраторских идентификаторов в соответствии с возможностями конфигурации системы;

h) для стандартных администраторских идентификаторов при коллективном их использовании должна обеспечиваться конфиденциальность секретной информации для аутентификации (например, частая смена паролей, а также максимально их быстрая смена при уходе пользователя с привилегированными правами или изменении его обязанностей, передача их всем пользователям с привилегированными правами посредством соответствующих механизмов).

Дополнительная информация

Несоответствующее использование привилегий, связанных с администрированием системы (любой функции или службы информационной системы, которая позволяет пользователю изменить средства управления системой или приложением) является основным фактором сбоев и нарушения функционирования системы.

9.2.4 Управление секретной информацией аутентификации пользователей

Метод реализации

Присваивание секретной информации аутентификации должно быть контролируемым через формализованный процесс управления.

Рекомендации по применению

Этот процесс должен включать в себя следующие требования:

a) пользователи должны подписать соглашение, по которому обязуются сохранять конфиденциальность личной секретной информации аутентификации и сохранять групповую (т.е. используемую несколькими пользователями) секретную информацию аутентификации исключительно в пределах группы; такое подписанное соглашение может быть частью трудового соглашения;

b) в тех случаях, когда пользователи должны сами обеспечивать сохранность своей секретной аутентификационной информации, им в начале должна быть выдана временная секретная информация аутентификации, которую они должны изменить на первом сеансе;

c) должны быть установлены процедуры проверки идентичности пользователя перед выдачей новой или заменой секретной аутентификационной информации, а также при выдаче временной секретной аутентификационной информации;

d) временная секретная информация аутентификации должна передаваться пользователю безопасным способом; следует избегать использования внешних сторон или незащищенных (открытым текстом) сообщений электронной почты;

e) временная секретная аутентификационной информация должна быть уникальной для конкретного пользователя и не должна быть легко угадываемой;

f) пользователи должны подтвердить получение секретной информации аутентификации;

g) секретная аутентификационная информация, установленная по умолчанию производителем, должна быть изменена после установки системы или программного обеспечения.

Дополнительная информация

Пароли являются широко применяемой разновидностью секретной аутентификационной информации и типовым средством проверки подлинности пользователя. Другим видом секретной информации аутентификации являются криптографические ключи, а также иные данные, сохраняемые на аппаратных ключах (например, смарт-карте), которые генерируют аутентификационные коды.

9.2.5 Пересмотр прав доступа пользователей

Метод реализации

Владельцы активов должны пересматривать права доступа пользователей через регулярные промежутки времени.

Рекомендации по применению

При пересмотре прав доступа должно учитываться следующее:

a) права доступа пользователей должны пересматриваться как через определенные интервалы времени, так и после изменений, таких как повышение или понижение в должности, или прекращение трудовых отношений (см. раздел 7);

b) права доступа пользователя должны пересматриваться и переназначаться в случае изменения его роли в организации;

c) привилегированные права доступа должна пересматриваться чаще;

d) назначенные привилегии должны проверяться через регулярные промежутки времени, чтобы гарантировать, что никто не получил привилегий несанкционированным образом;

e) изменения в привилегированных аккаунтах должны регистрироваться для периодического пересмотра.

Дополнительная информация

Этот метод реализации призван компенсировать возможные слабые места в выполнении методов реализации в п.п. 9.2.1, 9.2.2 и 9.2.6.

9.2.6 Отмена или изменение прав доступа

Метод реализации

Права доступа к информации и устройствам обработки информации всех сотрудников и внешних пользователей должны быть отменены после завершения трудовых отношений, контракта или соглашения.

Рекомендации по применению

После завершения трудовых отношений права доступа пользователя к информации и активам, связанным с устройствами обработки информации и службами, должны быть отменены или приостановлены. Изменения в должности должны находить отражение в отмене всех прав доступа, которые не были одобрены для новой позиции. Права доступа, которые должны быть отменены или скорректированы, распространяются также на физический и логический доступ. Отмена или корректировка могут быть выполнены посредством удаления, отмены или замены ключей, идентификационных карт, устройств обработки информации или абонементов. Любая документация, которая указывает права

доступа сотрудника или работающего по контракту, должна отражать отмену или корректировку прав доступа. Если уходящий сотрудник или внешней пользователь знает пароли для остающихся активными логинов пользователей, эти пароли должны быть изменены после завершения или изменения трудоустройства, контракта или соглашения.

Права доступа к информации и активам, связанным с устройствами обработки информации, должны быть понижены или отменены до прекращения трудовых отношений или их изменения, в зависимости от оценки риска, связанного с такими факторами, как:

a) было ли изменение или прекращение трудовых отношений инициировано работником, внешним пользователем или руководством, а также причины прекращения отношений;

b) текущие обязанности сотрудника, внешнего пользователя или иного другого пользователя;

c) ценность активов, находящихся в текущем доступе.

Дополнительная информация

В определенных обстоятельствах права доступа могут быть назначены более широкому кругу людей, нежели уходящие сотрудники или внешние пользователи, например, идентификационные данные группы. В таком случае уходящие сотрудники должны быть исключены из любого списка групповых прав доступа и должны быть приняты меры, чтобы уведомить всех других сотрудников и внешних пользователей о том, чтобы не передавать более эту информацию уходящему.

В том случае, когда прекращение отношений инициировано руководством, недовольные сотрудники или внешние пользователи могут намеренно повредить информацию или препятствовать работе средств обработки информации. Уволившиеся или уволенные сотрудники могут попытаться скопировать информацию для будущего использования.

9.3 Обязанности пользователей

Задача: сделать пользователей ответственными за сохранение их информации аутентификации.

9.3.1 Использование секретной информации аутентификации

Метод реализации

Пользователи обязаны следовать правилам организации при использовании секретной аутентификационной информации.

Рекомендации по применению

Всем пользователям должно быть рекомендовано:

a) сохранять конфиденциальность секретной аутентификационной информации, гарантируя, что она не будет разглашена никакой другой стороне, включая представителей органов власти;

b) избегать записывать (например, на листке бумаги, в файлах или мобильных устройствах) секретную аутентификационную информацию, кроме тех случаев, когда эти записи могут быть надежно сохранены и используется одобренный способ записи (например, программа Password Vault);

c) сменить секретную аутентификационную информацию в том случае, когда есть какие-либо признаки ее возможной компрометации;

d) в тех случаях, когда в качестве секретной информации аутентификации используются пароли, задавать стойкие пароли с достаточной минимальной длиной, которые

   1) легко запоминаются;

2) не используют такого, о чем любой может легко догадаться или вычислить на основе личной информации, например, имен, номеров телефонов, дат рождения и т.д.;
3) неуязвимы для словарной атаки (т.е. не состоит из слов, включенных в словари);
4) не содержит последовательности одинаковых цифр или символов;
5) будучи временными, меняются в первой же сессии;

e) не делиться секретной аутентификационной информацией;
f) обеспечивать надлежащую защиту паролей в тех случаях, когда пароли используются в качестве секретной аутентификационной информации в автоматизированных процедурах входа и хранятся в системе;
g) не использовать один и тот же пароль для деловых и частных целей.

Дополнительная информация

Применение технологии единого входа в систему (SSO) или других средств управления секретной информацией аутентификации снижает объем секретной аутентификационной информации, которая требуется от пользователя для защиты, и, таким образом, может увеличивать результативность рассматриваемого метода реализации. Однако, такие инструменты могут также усугублять последствия раскрытия секретной аутентификационной информации.

9.4 Контроль доступа к системе и приложениям

Задача: предотвратить несанкционированный доступ к системам и приложениям

9.4.1 Ограничения доступа к информации

Метод реализации

Доступ к информации и функциям прикладных систем должен быть ограничен в соответствии с политикой контроля доступа.

Рекомендации по применению

Ограничения доступа должны основываться на требованиях конкретных бизнес-приложений и соответствовать установленной политике контроля доступа.

Для обеспечения выполнения требований по ограничению доступа должно быть принято во внимание следующее:

a) предоставление меню для управления доступом к функциям системного приложения;
b) проверка, к каким данным может иметь доступ конкретный пользователь;
c) проверка прав доступа пользователя, например, на чтение, удаление или выполнение;
d) проверка прав доступа других приложений;
e) ограничения на информацию, содержащуюся в результатах работы приложения;
f) обеспечение физических и логических средств контроля доступа для изолирования уязвимых приложений, данных или систем.

9.4.2 Безопасные процедуры входа в систему

Метод реализации

Там, где это требуется политикой контроля доступа, доступ к системам и приложениям должен осуществляться в соответствии с безопасной процедурой входа в систему.

Рекомендации по применению

Должны быть выбраны подходящие методы аутентификации для подтверждения введенной

идентификационной информации пользователя.

Там, где требуется строгая проверка аутентификационной и идентификационной информации, должны быть использованы дополнительные меры аутентификации, такие как криптографические средства, смарт-карты, аппаратные ключи или биометрические средства.

Процедуры для входа в систему или приложение должны быть разработаны так, чтобы минимизировать возможность несанкционированного доступа. Т.е. процедуры входа должны предоставлять минимум информации о системе или приложении во избежание оказания нечаянной помощи неавторизованному пользователю. Надлежащая процедура входа должна:

a) не отображать идентификаторы системы или приложения до тех пор, пока процесс входа не завершен успешно;

b) выводить общее предупреждение, что доступ к компьютеру предоставляется только авторизованным пользователям;

c) не давать подсказок во время процедуры входа, которые могли бы помочь неавторизованному пользователю;

d) осуществлять подтверждение информации для входа только после завершения ввода данных. При обнаружении ошибки система не должна указывать, какая часть данных верна или неверна;

e) защищать от попыток входа методом полного перебора (или «грубой силы» - brute force);

f) регистрировать неуспешные и успешные попытки;

g) фиксировать инцидент безопасности при обнаружении попыток или факта успешного нарушения процедур входа;

h) отображать следующую информацию после успешного завершения процедуры входа:

    1) дата и время предыдущего успешного входа;

    2) детали всех неудачных попыток входа с момента последнего успешного входа;

i) не отображать вводимый пароль;

j) не передавать пароль открытым текстом по сети;

k) завершать неактивную сессию после определенного периода простоя, особенно если есть высокий риск, связанный с местонахождением, например, в общественном месте или за пределами действия системы менеджмента безопасности организации, или работой с мобильного устройства;

l) ограничивать время соединения для обеспечения дополнительной защиты приложениям с высоким риском и снижения возможности несанкционированного доступа.

Дополнительная информация

Пароли представляют собой широко применяемый способ обеспечения идентификации и авторизации, основанный на использовании информации, которую знает только пользователь. Тот же результат может быть получен при использовании криптографических методов и протоколов авторизации. Строгость процедуры авторизации пользователя должна соответствовать категории информации, к которой осуществляется доступ.

Если пароли передаются по сети открытым текстом во время процедуры входа, они могут быть перехвачены сетевыми программами анализа трафика (sniffers).

9.4.3 Система управления паролями

Метод реализации

Системы управления паролями должны быть диалоговыми и гарантировать пароли надлежащего качества.

Рекомендации по применению

Система управления паролями должна:

a) принуждать каждого пользователя использовать идентификационные данные и пароли для обеспечения отслеживаемости;

b) позволять пользователю выбирать и менять свои собственные пароли и включать процедуру подтверждения для обеспечения возможности исправления ошибок ввода;

c) вынуждать использовать пароли надлежащего качества;

d) принудительно заставлять пользователей менять пароли в ходе первой сессии;

e) заставлять регулярно или по мере необходимости менять пароли;

f) сохранять ранее использованные пароли и не допускать их повторного использования;

g) не отображать вводимые пароли;

h) хранить файлы с паролями отдельно от данных прикладной системы;

i) хранить и передавать данные в защищенном виде.

Дополнительная информация

Некоторые приложения требуют, чтобы пароли пользователя были назначены независимым администратором; в таких случаях вышеприведенные пункты b), d) и e) не применимы. В большинстве случаев пароли выбираются и меняются пользователями.

9.4.4 Использование утилит с привилегированными правами

Метод реализации

Использование утилит, которые могли бы обходить средства контроля системы и приложений, должно быть ограничено и жестко контролироваться.

Рекомендации по применению

Должны быть учтены следующие рекомендации по использованию утилит, которые могли бы обходить средства контроля системы и приложений:

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

b) отделение утилит от прикладного программного обеспечения;

c) ограничение использования утилит минимально возможным на практике числом доверенных, авторизованных пользователей (см. 9.2.3);

d) авторизация в каждом конкретном случае использования утилит;

e) ограничение доступности утилит, например, в период санкционированного изменения;

f) регистрация всех случаев использования утилит;

g) установление и документирование уровней авторизации для утилит;

h) удаление или отключение всех ненужных утилит;

i) не делать утилиты доступными тем пользователям, у которых имеется доступ к приложениям в системах, где требуется разделение обязанностей.

Дополнительная информация

На большинстве компьютеров установлена одна или более утилит, которые могли бы обходить средства контроля системы и приложений.

9.4.5 Контроль доступа к исходным кодам

Метод реализации

Доступ к исходному коду программ должен быть ограничен.

Рекомендации по применению

Доступ к исходному коду программ и связанным с ним элементам (таким, как схемы, спецификации, планы верификации и валидации) должен быть строго контролируемым с целью предотвращения включения в него несанкционированной функциональности и избежания непреднамеренных изменений, равно как и для сохранения конфиденциальности ценной интеллектуальной собственности. В отношении исходного кода это может быть достигнуто контролируемым централизованным хранением такого кода, предпочтительно в библиотеках исходных кодов. Следующие рекомендации должны быть приняты во внимание для контроля доступа к таким библиотекам исходных кодов с целью снижения возможности внесения искажений в компьютерные программы:

a) там, где это возможно, библиотеки исходных кодов не должны содержаться в рабочих системах;

b) исходные коды и библиотеки исходных кодов должны управляться в соответствии с установленными процедурами;

c) персонал технической поддержки не должен иметь неограниченного доступа к библиотекам исходных кодов;

d) обновление библиотек исходных кодов и связанных с ними элементов, а также выдача исходного кода программистам должно выполняться только после прохождения соответствующей авторизации;

e) листинги программ должны храниться в безопасной среде;

f) должны сохраняться записи всех обращений к библиотекам исходных кодов;

g) обслуживание и копирование библиотек исходных кодов должно проводиться по строгим процедурам контроля изменений (см. 14.2.2).

Если исходный код программы предполагается публиковать, то должны быть приняты во внимание дополнительные меры контроля для гарантии его целостности (например, цифровая подпись).

10 Криптография

10.1 Криптографические методы защиты

Задача: гарантировать надлежащее и результативное использование криптографии для защиты конфиденциальности, подлинности и/или целостности информации.

10.1.1 Политика использования криптографических методов защиты

Метод реализации

Должна быть разработана и внедрена политика использования криптографических методов для защиты информации.

Рекомендации по применению

При разработке политики в области криптографии следует учесть следующее:

a) подход к управлению применением криптографических методов в рамках всей организации, включая общие принципы, на которых должна быть основана защита бизнес-информации;

b) должен быть определен, основываясь на оценке рисков, требуемый уровень защиты с учетом типа, стойкости и качества необходимого криптографического алгоритма;

c) использование шифрование для защиты информации при передаче через мобильные или съемные носители или по линиям связи;

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

e) роли и обязанности, например, кто отвечает за:

    1) реализацию политики;

    2) управление ключами, включая их генерацию (см. 10.1.2);

f) стандарты, которые должны быть приняты в целях результативного применения в рамках всей организации (какое решение для какого бизнес-процесса используется);

g) влияние применения шифрования информации на инструменты, которые связаны с контролем содержания (например, обнаружение вредоносного кода).

При реализации криптографической политики организации необходимо учитывать регламенты и требования национальных органов, которые могут быть применены в области использования криптографических методов в различных странах, а также проблемы трансграничной передачи шифрованной информации (см. 18.1.5).

Криптографические методы могут быть использованы для достижения различных целей, связанных с защитой информации, например:

a) конфиденциальность: использование шифрования для защиты уязвимой или важной информации, хранящейся или передаваемой;

b) целостность/подлинность: использование цифровых подписей или кодов аутентичности сообщения для проверки подлинности или целостности сохраненной или передаваемой уязвимой или важной информации;

c) неопровержимость: использование криптографических методов для обеспечения свидетельств наступления или отсутствия события или действия;

d) аутентификация: использование криптографических методов для аутентификации пользователей и иных компонентов системы, запрашивающих доступ к пользователям системы, компонентам и ресурсам или взаимодействующих с ними.

Дополнительная информация

Формирование представления, насколько подходит то или иное криптографическое решение, должно рассматриваться как часть более широкого процесса оценки риска и выбора средств реализации. Такая оценка может затем быть использована для определения, является ли криптографический метод приемлемым, какая разновидность метода должна быть применена, для каких целей и какого бизнес-процесса.

Политика использования криптографических методов необходима для достижения максимальных выгод и минимизации рисков использования криптографических методов, а также чтобы избежать ненадлежащего или неправильного использования.

Необходимо обратиться за советом к специалисту в выборе соответствующих криптографических методов для достижения целей политики информационной безопасности.

10.1.2 Управление ключами

Метод реализации

Политика использования, защиты и срока действия криптографических ключей должна быть разработана и применяться в течение всего жизненного цикла ключей.

Рекомендации по применению

Политика должна содержать требования к управлению криптографическими ключами на протяжении всего их жизненного цикла, включая генерацию, хранение, архивирование, восстановление, распределение, аннулирование и уничтожение ключей.

Все криптографические ключи должны быть защищены от модификации или потери. Кроме этого, секретные и персональные ключи требуют защиты от несанкционированного использования, равно как и от раскрытия. Оборудование, применяемое для генерации, хранения и архивирования ключей должно быть физически защищено.

Система управления ключами должна базироваться на согласованном комплексе стандартов, процедур и методов обеспечения безопасности для:

a) генерации ключей для различных криптографических систем и приложений;

b) выпуска и получения сертификатов открытого ключа;

c) распределения ключей тем, кому они предназначены, включая и то, как они должны быть активированы после получения;

d) хранения ключей, включая то, как авторизованные пользователи будут получать доступ к ключам;

e) изменения или обновления ключей, в том числе и правила, определяющие, когда ключи должны быть изменены и как это должно быть сделано;

f) действий с скомпрометированными ключами;

g) аннулирования ключей, включая то, как ключ должен быть аннулирован или деактивирован, например, когда ключи были скомпрометированы или когда пользователь покидает организацию (в этом случае ключи должны быть архивированы);

h) восстановления утерянных или поврежденных ключей;

i) резервного копирования или архивирования ключей;

j) уничтожения ключей;

k) регистрации и аудита деятельности, связанной с управлениями ключами.

Для того, чтобы уменьшить вероятность несоответствующего использования должны быть определены даты активации и деактивации ключей так, чтобы ключи могли быть использованы только в период, определенный в соответствующей политике управления ключами.

Кроме того, для более надежного управления секретными и персональными ключами должна проверяться подлинность открытых ключей. Процесс аутентификации может быть выполнен посредством сертификатов открытых ключей, которые, обычно, выпускаются центром сертификации, который должен быть признанной организацией с соответствующими реализованными средствами управления и процедурами для обеспечения требуемого уровня доверия.

Соглашения об уровне обслуживания или контракты с внешними поставщиками

криптографических услуг, например, центрами сертификации, должны включать в себя вопросы ответственности, надежности услуг и времени отклика при оказании услуги (см. 15.2).

Дополнительная информация

Управление криптографическими ключами является принципиально важным с точки зрения результативного использования криптографических методов. Стандарт ISO/IEC 11770 [2][3][4] содержит детальную информацию по управлению ключами.

Криптографические методы также могут быть использованы для защиты криптографических ключей. Возможно, могут потребоваться процедуры для работы с юридическими запросами на доступ к криптографическим ключам, например, зашифрованная информация может быть затребована для расшифровки и использования в качестве свидетельства в суде.

11 Физическая защита и защита от внешних воздействий

11.1 Охраняемые зоны

Задача: предотвратить несанкционированный физический доступ, повреждение и воздействие на информацию и средства для обработки информации организации.

11.1.1 Физический периметр безопасности

Метод реализации

Периметры безопасности должны быть определены и использоваться для защиты зон нахождения уязвимой или особо важной информации и средств для обработки информации.

Рекомендации по применению

При формировании физических периметров безопасности должны быть приняты во внимание и выполнены, где это возможно, следующие рекомендации:

a) периметры безопасности должны быть определены, а расположение и степень защиты, обеспечиваемой периметрами, должна зависеть от требований по безопасности активов внутри периметра и результатов оценки рисков;

b) периметры зданий и мест нахождения устройств обработки информации должны быть физически прочными (т.е. не должны иметь в периметре разрывов или зон, где он может быть легко преодолен); внешнее перекрытие, стены и пол должны иметь монолитную конструкцию, а все внешние двери должны быть соответствующим образом защищены от несанкционированного доступа охранными средствами (например, засовы, сигнализация, замки); двери и окна должны быть закрыты, пока помещение находится без присмотра, а внешняя защита должна включать и окна, особенно, на первом этаже;

c) должны функционировать обслуживаемые зоны приема или иные средства контроля физического доступа к определенным местам и зданиям; доступ к определенным местам и зданиям должен быть ограничен и разрешен только авторизованному персоналу;

d) должны быть выстроены, где это возможно, физические преграды для защиты от неавторизованного физического доступа и внешнего загрязнения;

e) все пожарные выходы по периметру должны быть оснащены сигнализацией, быть под наблюдением и проверены в местах соединения со стенами, чтобы обеспечить требуемый уровень защищенности в соответствии с действующими региональными, национальными и международными стандартами; они должны безотказно функционировать в соответствии с местными правилами пожарной безопасности;

f) должны быть установлены подходящие системы обнаружения проникновения, соответствующие региональным, национальным или международным стандартам, и регулярно проверяться на предмет того, что ими охвачены все внешние двери и доступные окна; неиспользуемые площади должны быть оснащены постоянно работающей сигнализацией; защита также должна быть обеспечена и для других зон, например, компьютерного зала или серверных;

g) оборудование обработки информации, находящееся под управлением организации, должно быть отделено от оборудования, управляемого внешними сторонами.

Дополнительная информация

Физическая защита может быть обеспечена введением одной или нескольких линий защиты вокруг помещений организации и устройств обработки информации. Применение множественных линий защиты дает дополнительную защиту, так как сбой на одной не ведет к тому, что безопасность будет немедленно нарушена.

Охраняемой зоной может быть запираемый офис или несколько помещений, окруженных непрерывной внутренней линией защиты. Могут быть необходимы дополнительные линии защиты и периметры для контроля физического доступа между зонами с различными требованиями по безопасности внутри периметра безопасности. Особое внимание к безопасному физическому доступу должно быть уделено в том случае, когда в здании размещаются активы многих организаций.

Применение мер физического контроля, особенно для охраняемых зон, должно быть увязано с техническими и экономическими обстоятельствами организации, как это следует из оценки рисков.

11.1.2 Средства контроля прохода

Метод реализации

Охраняемые зоны должны быть защищены соответствующими средствами контроля прохода с целью гарантировать, что только имеющему права персоналу разрешен проход.

Рекомендации по применению

a) дата и время прихода и ухода посетителей должно регистрироваться, а также посетители должны сопровождаться, если только их приход не был заранее согласован; им должен быть предоставлен проход только для конкретных и одобренных целей, они должны быть проинструктированы по требованиям безопасности данной зоны и процедурам действий в чрезвычайной ситуации. Идентичность посетителей должна быть установлена соответствующими методами;

b) доступ в зоны, где обрабатывается или хранится конфиденциальная информация, должен быть ограничен только авторизованными посетителями применением соответствующих средств контроля прохода, например, использованием механизма идентификации по двум признакам, таким как карточка доступа и секретный PIN-код;

c) должен надежным образом вестись и проверяться рукописный или электронный журнал всех посещений;

d) все сотрудники и работающие по контракту, в также посетители обязаны носить определенные знаки визуальной идентификации и должны немедленно сообщать в службу безопасности, если встретили посетителей без сопровождения и кого-то без знака визуальной идентификации;

e) персонал внешних служб обеспечения и только в случае необходимости должен иметь ограниченный доступ к охраняемым зонам или оборудованию, обрабатывающему

конфиденциальную информацию; этот доступ должен быть авторизован и контролироваться;

f) права доступа к охраняемым зонам должны регулярно пересматриваться и обновляться, а также отменяться в случае необходимости (см. 9.2.5 и 9.2.6).

11.1.3 Защита офисов, помещений и оборудования

Метод реализации

Меры защиты для офисов, помещений и оборудования должны быть разработаны и применяться.

Рекомендации по применению

Для защиты офисов, помещений и оборудования должны быть приняты к сведению следующие рекомендации:

a) критически важное оборудование должно быть размещено так, чтобы исключить открытый доступ;

b) там, где это применимо, здания должны быть незаметными и давать минимум информации о своем назначении, без явных признаков – снаружи или внутри здания – позволяющих сделать вывод о наличии деятельности по обработке информации;

c) оборудование должно быть сконфигурировано таким образом, чтобы конфиденциальная информация или действия не были видимы и слышимы снаружи. При необходимости, должно быть предусмотрено электромагнитное экранирование;

d) справочники и внутренние телефонные книги, содержащие информацию о размещении обрабатывающего информацию оборудования, не должны быть легко доступны для неавторизованных лиц.

11.1.4 Защита от внешних угроз и угроз природного характера

Метод реализации

Должны быть разработаны и применяться меры физической защиты от стихийных бедствий, злонамеренных действий или аварий.

Рекомендации по применению

Следует проконсультироваться со специалистом, каким образом избежать повреждений от пожара, наводнения, землетрясения, взрыва, общественных беспорядков и других форм угроз природного, техногенного или социального характера.

11.1.5 Работа в охраняемых зонах

Метод реализации

Должны быть разработаны и применяться процедуры для работы в охраняемой зоне.

Рекомендации по применению

Должны быть учтены следующие рекомендации:

a) о существовании охраняемой зоны или деятельности в ней должен знать только тот персонал, которому это положено знать в силу служебных обязанностей;

b) в охраняемых зонах для обеспечения безопасности и предотвращения злонамеренных действий должна быть исключена работа без сопровождения;

c) безлюдные охраняемые зоны должны быть физически закрыты и периодически осматриваться;

d) фото-, видео-, аудио- и иная записывающая аппаратура, такая как камеры в мобильных

устройствах, должны быть запрещены без специального разрешения.

Меры по работе в охраняемых зонах включают в себя меры для сотрудников и внешних пользователей, работающих в охраняемой зоне, и охватывают все виды деятельности, выполняемые в охраняемой зоне.

11.1.6 Зоны доставки и отгрузки

Метод реализации

Места доступа, такие как зоны доставки и отгрузки и иные, где есть возможность пройти в помещение лицам без соответствующих прав, должны контролироваться и, если возможно, быть изолированными от средств обработки информации, чтобы избежать несанкционированного доступа.

Рекомендации по применению

Должны быть учтены следующие рекомендации:

a) доступ к зоне доставки и отгрузки с внешней стороны здания должен быть ограничен идентифицированным и имеющим разрешение персоналом;

b) зона доставки и отгрузки должна быть сформирована так, чтобы прием и отправка могли быть осуществлены без доступа курьера к другим частям здания;

c) наружные двери зоны доставки и отгрузки должны быть закрыты в то время, когда внутренние открыты;

d) полученные материалы должны быть осмотрены и проверены на наличие взрывчатых веществ, химикатов и иных опасных материалов до того, как будут перемещены из зоны доставки и отгрузки;

e) полученные материалы должны быть зарегистрированы на входе в соответствии с процедурами управления активами (см. раздел 8);

f) получаемые и отправляемые посылки должны быть физически отделены друг от друга, если это возможно;

g) полученные материалы должны быть осмотрены на предмет наличия следов вскрытия в пути. Если такие свидетельства обнаружены, необходимо немедленно сообщить сотрудникам службы безопасности.

11.2 Оборудование

Задача: предотвратить потерю, повреждение, кражу или компрометацию активов и нарушение деятельности организации.

11.2.1 Размещение и защита оборудования

Метод реализации

Оборудование должно быть размещено и защищено так, чтобы снизить риски, связанные с природными угрозами и опасностями, а также возможностью несанкционированного доступа.

Рекомендации по применению

Для защиты оборудования должны быть приняты во внимание следующие рекомендации:

a) оборудование должно быть размещено так, чтобы свести к минимуму входы в рабочую зону без необходимости;

b) обрабатывающее информацию оборудование, оперирующее с критически важными данными, должно размещаться таким образом, чтобы снизить риск того, что лица, не

имеющие разрешения, увидят информацию в процессе ее обработки;

c) устройства хранения информации должны быть защищены от неавторизованного доступа;

d) объекты, требующие специальных мер защиты, должны охраняться, чтобы понизить общий уровень требуемой защиты;

e) должны быть предприняты меры для снижения риска потенциальных угроз физического и природного характера, например, кражи, пожара, взрывов, задымления, наводнения (или залива водой из-за аварии), запыления, вибрации, химического воздействия, прерывания электроснабжения и связи, электромагнитной радиации и вандализма;

f) должны быть установлены правила приема пищи и курения в зонах, расположенных рядом с оборудованием обработки информации;

g) должны отслеживаться условия эксплуатации, такие как температура и влажность, для контроля факторов, которые могли бы негативно повлиять на работу оборудования обработки информации;

h) должна быть обеспечена молниезащита всех зданий и должны быть установлены устройства защиты от перенапряжения на всех входящих силовых и коммуникационных линиях;

i) должна быть рассмотрена возможность применения специальных мер защиты, таких как клавиатурные мембраны, для оборудования, работающего в производственных условиях;

j) для оборудования, обрабатывающего конфиденциальную информацию, должна быть предусмотрена защита, снижающая риск утечки информации через электромагнитное излучение.

11.2.2 Службы обеспечения

Метод реализации

Оборудование должно быть защищено от перебоев в электроснабжении и других нарушений, вызванных перебоями в работе служб обеспечения.

Рекомендации по применению

Службы обеспечения (например, энергоснабжения, телекоммуникаций, водо- и газоснабжения, канализации, вентиляции и кондиционирования) должны:

a) соответствовать требованиям поставщика оборудования и местным законодательным требованиям;

b) должны регулярно оцениваться с точки зрения их способности соответствовать развитию бизнеса и взаимодействия с другими службами обеспечения;

c) регулярно проверяться для гарантии их надлежащего функционирования;

d) в случае необходимости, иметь сигнализацию о неисправности;

e) в случае необходимости, иметь несколько дистанционно разделенных линий подачи.

Должны быть обеспечены аварийное питание и связь. Аварийные выключатели и вентили для отключения электричества, воды, газа и других видов снабжения должны располагаться вблизи аварийных выходов или помещений с оборудованием.

Дополнительная информация

Дублирование сетевых соединений может быть обеспечено несколькими каналами связи от более, чем одного провайдера услуг.

11.2.3 Защита кабельных сетей

Метод реализации

Питающие кабели и кабели, передающие данные или обеспечивающие работу информационных сервисов, должны быть защищены от перехвата, помех или повреждения.

Рекомендации по применению

Для защиты кабельных сетей должны быть приняты во внимание следующие рекомендации:

a) телекоммуникационные линии и линии питания устройств обработки информации должны быть подземными, где это возможно, или же иметь соответствующую дополнительную защиту;

b) кабели питания и телекоммуникационные кабели должны быть проложены отдельно для исключения помех;

c) для уязвимых и критически важных систем должны быть предусмотрены дополнительные меры, включая:

   1) прокладку армированного кабеля, расположение точек входа кабеля в запирающихся помещениях или ящиках;

   2) применение электромагнитных экранов для защиты кабелей;

   3) проведение проверок техническими средствами и на местах для обнаружения устройств, подключенных к кабелям;

   4) контролируемый доступ к соединительным панелям и коммутационным комнатам.

11.2.4 Обслуживание оборудования

Метод реализации

Оборудование должно надлежащим образом обслуживаться, чтобы гарантировать его постоянную готовность и исправность.

Рекомендации по применению

При обслуживании оборудования должны быть приняты во внимание следующие рекомендации:

a) оборудование должно обслуживаться в соответствии с заданными производителем периодами обслуживания и требованиями;

b) ремонт и обслуживание оборудования должен выполнять только авторизованный обслуживающий персонал;

c) должны сохраняться записи обо всех предполагаемых или фактических сбоях, а также обо всех профилактических и ремонтных работах;

d) в тех случаях, когда планируется проведение обслуживания, должны быть приняты соответствующие меры с учетом того, будут ли проводиться работы на месте или во внешней организации; если необходимо, конфиденциальная информация должна быть удалена из оборудования или обслуживающий персонал должен иметь соответствующий допуск;

e) все требования к обслуживанию, налагаемые договорами страхования, должны быть выполнены;

f) перед возвращением оборудования в эксплуатацию должна быть проведена проверка, чтобы гарантировать, что в оборудование не внесены незаконные изменения и оно функционирует нормально.

11.2.5 Вынос активов

Метод реализации

Оборудование, информация или программное обеспечение не должны выноситься за пределы территории без предварительного разрешения.

Рекомендации по применению

Должны быть приняты во внимание следующие рекомендации:

a) должны быть определены сотрудники и внешние пользователи, кто имеет право выдавать разрешения на вынос активов;

b) должны быть установлены сроки возврата актива и затем проверено их соблюдение;

c) в тех случаях, когда необходимо и возможно, вынос и возврат актива должны быть зарегистрированы;

d) личность, должность и принадлежность лица, которое управляет активами или использует их, должны быть документированы и эти документы должны быть возвращены вместе с оборудованием, информацией или программным обеспечением.

Дополнительная информация

Выборочные проверки, проводимые для выявления случаев несанкционированного выноса активов, могут также проводиться для выявления неразрешенных записывающих устройств, оружия, а также для предупреждения их проноса на территорию и выноса с территории. Такие выборочные проверки должны проводиться в соответствии с действующим законодательством и регламентами. Персонал должен быть информирован о том, что проводятся выборочные проверки, и эти проверки должны проводиться в строгом соответствии с законодательными и нормативными требованиями.

11.2.6 Защита оборудования и активов вне территории

Метод реализации

Меры обеспечения безопасности должны применяться к активам вне территории, принимая во внимание различные риски работы вне помещений организации.

Рекомендации по применению

Использование за пределами организации любого оборудования, обрабатывающего или хранящего информацию, должно быть разрешено руководством. Это относится к оборудованию как принадлежащему организации, так и к личному, но используемому в интересах организации.

Для защиты оборудования вне организации должны быть приняты во внимание следующие рекомендации:

a) оборудование и носители, выносимые за пределы организации, не должны оставляться без присмотра в общественных местах;

b) инструкции производителя по защите оборудования должны всегда соблюдаться, например, защита от воздействия сильных электромагнитных полей;

c) меры для работы вне офиса, таких как работа дома, удаленная работа или работа на временном месте, должны быть определены на основе оценки рисков и применены соответствующие ситуации методы, например, запирающиеся шкафы для хранения документов, политика чистого стола, контроль доступа к компьютерам и защита линий связи с офисом (см. также ISO/IEC 27033 [15][16][17][18][19]);

d) в тех случаях, когда оборудование, находящееся вне территории организации, передается друг другу различными людьми или внешними сторонами, должен вестись журнал,

который регистрирует всю последовательность передачи оборудования, включая, как минимум, фамилии и названия организаций тех, кто несет ответственность за оборудование.

Риски, связанные, например, с повреждением, кражей или прослушиванием, могут существенно отличаться в зависимости от места и должны учитываться при определении наиболее подходящих мер.

Дополнительная информация

Оборудование, обрабатывающее или хранящее информацию, включает в себя все виды персональных компьютеров, органайзеров, мобильных телефонов, смарт-карт, бумажные документы и иные виды носителей, которые хранятся для работы дома или выносятся с обычного места работы.

Дополнительная информация о других аспектах защиты переносного оборудования может быть найдена в 6.2.

Возможно, будет целесообразно уменьшить риск, убедив определенных сотрудников не работать вне офиса или ограничив использование ими портативного ИТ-оборудования.

11.2.7 Безопасная утилизация или повторное использование оборудования

Метод реализации

Все элементы оборудования, содержащие накопители, должны быть проверены, чтобы гарантировать, что любые ценные данные и лицензионное программное обеспечение удалены или надежным образом затерты новой информацией до утилизации или повторного использования.

Рекомендации по применению

Оборудование должно быть проверено до утилизации или повторного использования с целью выяснить, содержатся ли в нем накопители или нет.

Накопители, содержащие конфиденциальную или защищенную авторскими правами информацию должны быть физически разрушены или информация должна быть стерта, удалена или перезаписана с применением технологий, делающих невозможным восстановление оригинальной информации, а не использованием стандартных функций удаления или форматирования.

Дополнительная информация

Для поврежденного оборудования, содержащего носители, может потребоваться оценка рисков, чтобы определить, должен ли быть этот элемент скорее уничтожен, нежели отдан в ремонт или выброшен. Информация может быть скомпрометирована из-за ненадлежащей утилизации или повторного применения оборудования.

Кроме того, для надежной очистки диска шифрование всей информации на диске снижает риск раскрытия конфиденциальной информации в тех случаях, когда оборудование идет на утилизацию или повторное использование при условии, что:

a) шифрование достаточно сильное и охватывает весь диск (включая незанятые части кластеров, своп-файлы и т.д.);

b) ключи шифрования достаточно длинные, чтобы противостоять атакам методом подбора;

c) ключи шифрования сами хранятся надежно (например, никогда не хранятся на том же диске).

Более детальные рекомендации по шифрованию см. в разделе 10.

Методы надежной перезаписи накопителей отличаются в зависимости от технологии,

применяемой в носителях информации. Необходимо проанализировать инструменты перезаписи, чтобы убедиться, что они применимы к конкретной технологии.

11.2.8 Оборудование пользователя, оставленное без присмотра

Метод реализации

Пользователи должны гарантировать, что у оставленного без присмотра оборудования имеется соответствующая защита.

Рекомендации по применению

Все пользователи должны быть осведомлены о требованиях безопасности и процедурах для защиты оборудования, остающегося без присмотра, равно как и об их ответственности за обеспечение такой защиты. Пользователям должно быть рекомендовано:

a) разрывать активную сессию после завершения работы, если только она не может быть защищена соответствующим блокирующим механизмом, например, паролем скринсейвера;

b) выходить из приложений или сетевых служб, когда в них более нет необходимости;

c) защищать компьютеры или мобильные устройства от несанкционированного использования запиранием на ключ или схожим способом, например, доступом по паролю, когда устройство не используется.

11.2.9 Политика чистого стола и чистого экрана

Метод реализации

Должна быть установлена политика чистого стола для бумажных документов и сменных носителей информации, и политика чистого экрана для устройств обработки информации.

Рекомендации по применению

Политика чистого стола и чистого экрана должна учитывать категории информации (см. 8.2), законодательные и контрактные требования (см. 18.1), а также соответствующие риски и корпоративную культуру организации. Следует учесть следующие рекомендации:

a) уязвимая или критически важная для бизнеса информация, например, на бумаге или на электронных носителях, должна содержаться запертой (идеально – в сейфе или шкафу, или ином предмете мебели, обеспечивающем защиту), пока не используется, особенно, если в офисе никого нет;

b) компьютеры и терминалы, оставленные без присмотра, должны оставляться в состоянии выполненного выхода из системы или защищенными механизмом блокировки экрана и клавиатуры, управляемым паролем, аппаратным ключом или подобным средством аутентификации пользователя, и должны быть блокированы ключом, паролями или иными средствами, когда не используются;

c) не должно допускаться несанкционированное использование копировальных аппаратов и других воспроизводящих устройств (например, сканеров, цифровых камер);

d) отпечатки, содержащие уязвимую или классифицированную информацию, необходимо забирать из печатающих устройств немедленно.

Дополнительная информация

Политика чистого стола/чистого экрана снижает риск несанкционированного доступа, потери или повреждения информации в рабочее и внерабочее время. Сейфы и другие устройства надежного хранения могли бы также защитить хранимую в них информацию от таких угроз, как пожар, землетрясение, наводнение или взрыв.

Следует рассмотреть возможность использования печатающих устройств с функцией PIN-кода, когда только создатель документа может его получить, находясь непосредственно у принтера.

12 Безопасность производственной деятельности

12.1 Рабочие процедуры и обязанности

Задача: гарантировать надлежащую и безопасную эксплуатацию средств обработки информации.

12.1.1 Документированные рабочие процедуры

Метод реализации

Рабочие процедуры должны быть документированы и доступны всем пользователям, которым они необходимы.

Рекомендации по применению

Должны быть разработаны рабочие процедуры для повседневной деятельности, связанной с оборудованием обработки информации и средствами связи, такие, как процедуры включения и выключения компьютеров, резервного копирования, обслуживания оборудования, работы с носителями, управления и обеспечения безопасности в компьютерном зале и при обработке почты.

Эти рабочие процедуры должны содержать инструкции по выполнению действий, включая:

a) установку и конфигурацию систем;

b) ручную и автоматизированную обработку информации;

c) резервное копирование (см. 12.3);

d) требования к планированию, в том числе и с учетом связей с другими системами, срока начала первой работы и срока окончания последней;

e) инструкции по обработке ошибок или других исключительных ситуаций, которые могут возникнуть в ходе работы, включая ограничения на использование системных утилит (см. 9.4.4);

f) техническую поддержку и контакты для передачи проблемы на вышестоящий уровень, включая контакты внешних служб обеспечения, в случае отклонений от ожидаемого функционирования или возникновения технических сложностей;

g) инструкции по обращению с особыми носителями и особыми данными, например, по использованию специальных бланков или управлению выводом конфиденциальной информации, включая уничтожение результатов вывода в случае неудачного выполнения операции (см. 8.3 и 11.2.7);

h) перезапуск системы и процедуры восстановления в случае сбоя в системе;

i) управление информацией, содержащейся в журналах проверок и системных журналах (см. 12.4);

j) процедуры мониторинга.

Рабочие процедуры и документированные процедуры по системным операциям должны рассматриваться как официальные документы и изменения в них утверждаться руководством. Там, где это технически возможно, информационные системы должны управляться единым образом, с применением одних процедур, инструментов и утилит.

12.1.2 Управление изменениями

Метод реализации

Изменения в организации, бизнес-процессах, средствах для обработки информации и системах, которые влияют на информационную безопасность, должны быть управляемыми.

Рекомендации по применению

В частности, должно быть принято во внимание следующее:

a) идентификация и регистрация существенных изменений;

b) планирование и тестирование изменений;

c) оценка потенциального влияния осуществляемых изменений, включая влияние на информационную безопасность;

d) процедура официального утверждения предлагаемых изменений;

e) подтверждение, что требования по информационной безопасности выполнены;

f) информирование об изменениях всех заинтересованных лиц;

g) процедуры отката к начальному состоянию, включая процедуры и обязанности по остановке и восстановлению после неудачных изменений и непредвиденных событий;

h) наличие процесса срочных изменений для обеспечения быстрого и контролируемого выполнения изменений, необходимых для устранения инцидента (см. 16.1).

Должны быть разработаны формализованные процедуры управления и установлена ответственность для гарантии надлежащего контроля изменений. При выполнении изменений в контрольном журнале должна сохраняться вся необходимая информация.

Дополнительная информация

Несоответствующий контроль изменений в средствах обработки информации и системах является типичной причиной системных сбоев или нарушений безопасности. Изменения в операционной среде, особенно при переходе системы со стадии разработки на стадию эксплуатации, могут влиять на надежность приложений (см. 14.2.2).

12.1.3 Управление производительностью

Метод реализации

Использование ресурсов должно отслеживаться, регулироваться и делаться прогноз требований к производительности в будущем с тем, чтобы гарантировать необходимую работоспособность систем.

Рекомендации по применению

Требования к производительности должны быть определены с учетом важности рассматриваемой системы для бизнеса. Должны проводиться настройка и мониторинг системы, чтобы гарантировать и, где необходимо, улучшать пригодность и эффективность систем. Должны быть задействованы средства обнаружения для своевременного выявления проблем. Прогнозы требований к производительности в будущем должны учитывать новые требования как со стороны бизнеса, так и систем, а также текущие и прогнозируемые тенденции в возможностях обработки информации в организации.

Особое внимание требуется уделить ресурсам с длительным сроком получения или с высокой стоимостью; поэтому руководители должны отслеживать использование ключевых ресурсов системы. Они должны выявлять тенденции в использовании, особенно, связанные с бизнес-приложениями или инструментарием управления информационными системами.

Руководители должны использовать эту информацию для выявления и устранения

потенциальных узких мест и зависимостей от ключевого персонала, которые могут представлять угрозу безопасности систем или служб, а также планировать соответствующие действия.

Обеспечение достаточной производительности может быть достигнуто как увеличением возможностей, так и снижением запросов. Примеры управления запросами включают в себя:

a) удаление устаревших данных (объем диска);

b) деинсталляцию приложений, систем, баз данных или сред;

c) оптимизацию пакетных заданий и их расписания;

d) оптимизацию алгоритмов приложений или запросов к базам данных;

e) отказ в предоставлении или ограничение полосы пропускания для ресурсоемких служб, если они не важны для бизнеса (например, потоковое видео).

Должна быть рассмотрена возможность документированного плана управления производительностью для критически важных систем.

Дополнительная информация

Рассмотренные меры также применимы к человеческим ресурсам, равно как и к офисам и оборудованию.

12.1.4 Разделение среды разработки, тестирования и эксплуатации

Метод реализации

Среда разработки, тестирования и рабочая среда должны быть отделены друг от друга для снижения рисков несанкционированного доступа или изменений в рабочей среде.

Рекомендации по применению

Должен быть определен и реализован необходимый для предотвращения возникновения проблем функционирования уровень разделения среды разработки, тестирования и рабочей среды.

Должно быть принято во внимание следующее:

a) должны быть определены и документированы правила перевода программного обеспечения из статуса разработки в статус годности к эксплуатации;

b) среда разработки и рабочая среда должны быть запущены в разных системах или на разных компьютерах и в разных доменах или директориях;

c) изменения в рабочих системах и приложениях должны тестироваться в тестовой или промежуточной среде до того, как они будут применены к рабочим системам;

d) не должно проводиться тестирования на рабочих системах, кроме как в случае возникновения исключений;

e) компиляторы, редакторы и другой инструментарий для разработки или системные утилиты не должны быть доступны из рабочих систем, когда в этом нет необходимости;

f) пользователи должны использовать разные пользовательские профили для рабочих и тестовых систем и на экране должны отображаться соответствующие предупреждающие сообщения для снижения риска ошибки;

g) конфиденциальные данные не должны копироваться в среду тестирования систем, если только не обеспечены для тестируемой системы надлежащие средства контроля (см. 14.3).

Дополнительная информация

Действия в ходе разработки и тестирования могут вызывать серьезные проблемы,

например, нежелательное изменение файлов или системной среды, или системные сбои. Есть необходимость поддерживать понятную и стабильную среду для выполнения полноценного тестирования и предотвращения несанкционированного доступа разработчиков к рабочей среде.

Там, где персонал, выполняющий разработку и тестирование, имеет доступ к рабочей среде и ее информации, он может иметь возможность внедрить неавторизованный и не прошедший тестирование код или альтернативные рабочие данные. На некоторых системах такая возможность могла бы быть использована для совершения обмана или внедрения не протестированного или зловредного кода, что может вызвать серьезные проблемы в эксплуатации.

Персонал, выполняющий разработку и тестирование, также представляет угрозу для конфиденциальности рабочей информации. Действия в ходе разработки и тестирования могут вызывать ненамеренные изменения в программном обеспечении или информации, если они выполняются в одной вычислительной среде. Таким образом, желательно разделение среды разработки, тестирования и рабочей среды для снижения риска случайного изменения или неавторизованного доступа к рабочему программному обеспечению или рабочим данным (см. 14.3 о защите данных для тестирования).

12.2 Защита от вредоносного кода

Задача: гарантировать, что информация и средства обработки информации защищены от вредоносного кода.

12.2.1 Меры защиты от вредоносного кода

Метод реализации

В отношении вредоносного кода должны применяться меры по обнаружению, предупреждению и восстановлению с соответствующим информированием пользователей.

Рекомендации по применению

Защита от вредоносного кода должна основываться на применении программ обнаружения вредоносного кода и восстановления, осведомленности об информационной безопасности и соответствующих средствах контроля доступа к системе и управлению изменениями. Должны быть приняты во внимание следующие рекомендации:

a) разработка официальной политики, запрещающей использование неавторизованного программного обеспечения (см. 12.6.2 и 14.2);

b) внедрение мер, которые предотвращают или выявляют применение неавторизованного программного обеспечения (например, ведение списка разрешенных программ);

c) внедрение мер, которые предотвращают или выявляют обращение к известным вредоносным или подозрительным веб-сайтам (например, ведение черных списков таких сайтов);

d) разработка официальной политики для защиты от рисков, связанных с получением файлов и программного обеспечения из или через внешние сети или любые иные среды, с указанием, какие защитные меры должны быть предприняты;

e) уменьшение уязвимостей, которые могли бы быть использованы вредоносным кодом, например, посредством управления техническими уязвимостями (см. 12.6);

f) проведение регулярных проверок программного обеспечения и данных систем, поддерживающих важные бизнес-процессы; присутствие любых несанкционированных файлов и изменений должно официально расследоваться;

g) установка и регулярное обновление программ обнаружения вредоносного кода и восстановления для сканирования компьютеров и носителей в качестве предупредительной меры или на постоянной основе; сканирование должно выполняться, включая:

   1) сканирование на предмет вредоносного кода любых файлов, полученных по сети или через любые носители информации, до их использования;

   2) сканирование на предмет вредоносного кода вложений к сообщениям электронной почты и загруженных файлов до их использования; такое сканирование должно проводиться в различных местах, например, на почтовых серверах, настольных компьютерах и на аппаратуре подключения организации к сети;

   3) сканирование на предмет вредоносного кода веб-страниц;

h) определение обязанностей и процедур для обеспечения защиты от атак вредоносного кода, обучение их применению, составлению отчетов и восстановлению после атак вредоносного кода;

i) подготовка соответствующих планов обеспечения непрерывности бизнеса для восстановления после атак вредоносного кода, включая все необходимые данные и программы резервного копирования, а также мероприятия по восстановлению (см. 12.3);

j) выполнение процедур регулярного сбора информации, таких как подписка на рассылки или посещение ресурсов с информацией о новых вредоносных программах;

k) выполнение процедур проверки информации, связанной с вредоносными программами, и гарантирование того, что предупредительные сообщения точны и информативны; руководители должны гарантировать, что для отделения реальных вредоносных программ от ложных используются квалифицированные источники, например, авторитетные журналы, надежные Интернет-сайты или поставщики, производящие программное обеспечение для защиты от вредоносных программ; все пользователи должны быть извещены о проблеме ложных вредоносных программ и что необходимо делать при их получении;

l) изолирование сред, в которых последствия могут быть катастрофическими.

Дополнительная информация

Применение двух или более программных продуктов, защищающих от вредоносных программ в системах обработки информации, от разных производителей и реализующих разные технологии может повысить результативность защиты от вредоносного кода.

Необходимо озаботиться тем, чтобы вредоносный код не был внедрен в ходе обслуживания и действий в аварийной ситуации, которые могут производиться в обход обычных мер по защите от вредоносного кода.

Применение в качестве средства защиты от вредоносного кода только обнаруживающих и восстанавливающих программ обычно недостаточно и требуются дополнительные рабочие процедуры, которые предотвращают внедрение вредоносного кода.

12.3 Резервное копирование

Задача: обеспечить защиту от потери данных.

12.3.1 Резервное копирование информации

Метод реализации

Должно выполняться и регулярно тестироваться резервное копирование информации, программного обеспечения и образов системы в соответствии с принятой политикой

резервного копирования.

Рекомендации по применению

Должна быть установлена политика резервного копирования, чтобы определить требования организации к резервному копированию информации, программного обеспечения и систем.

Политика резервного копирования должна определять требования по защите и срокам хранения.

Должны быть предоставлены соответствующие устройства для резервного копирования с гарантией того, что существенная информация и программное обеспечение могут быть восстановлены после аварийной ситуации или сбоя носителя.

При формировании плана резервного копирования должно быть учтено следующее:

a) должны делаться точные и полные записи резервных копий и быть разработаны документированные процедуры восстановления;

b) объем (например, полное или частичное копирование) и частота резервного копирования должны соответствовать бизнес-требованиям организации, требованиям по безопасности сохраняемой информации, и важности этой информации для обеспечения непрерывности деятельности организации;

c) резервные копии должны храниться в удаленных местах, на существенном расстоянии для избежания повреждения в случае аварийных ситуаций в основном офисе;

d) резервируемой информации должен быть обеспечен соответствующий уровень защиты, как физической, так и от угроз внешнего воздействия (см. раздел 11), согласно стандартам, применяемым в основном офисе;

e) носители для резервных копий должны регулярно тестироваться для гарантии того, что на них можно положиться при применении в случае экстренной необходимости; это должно совмещаться с тестами процедур восстановления и проверкой на соответствие требуемому времени восстановления. Тестирование возможности восстановить сохраненные данные на выделенных для тестирования носителях, а не перезаписью информации на оригинальные носители в случае, если в процессе резервного копирования или восстановления произошел сбой или обнаружились невосстановимое повреждение или потеря данных;

f) в тех случаях, когда важна конфиденциальность, резервируемые данные должны быть защищены криптографическими средствами.

Рабочие процедуры должны предусматривать контроль выполнения резервного копирования и обработку сбоев в ходе производимого по графику резервного копирования, чтобы гарантировать завершение всех операций резервного копирования в соответствии с политикой резервного копирования.

Мероприятия по резервному копированию для конкретных систем или служб должны регулярно тестироваться для гарантии того, что они соответствуют требованиям плана по обеспечению непрерывности бизнеса. Для систем и служб, имеющих критически важное значение, мероприятия по резервному копированию должны охватывать всю системную информацию, приложения и данные, необходимые для восстановления всей системы в случае аварийной ситуации.

Должен быть определен срок хранения существенной для бизнеса информации с учетом любых требований к архивированию копий, которые должны постоянно сохраняться.

12.4 Ведение журналов и мониторинг

Задача: регистрировать события и обеспечивать свидетельства

12.4.1 Регистрация событий

Метод реализации

Должны вестись, сохраняться и регулярно анализироваться журналы, содержащие записи активности пользователей, возникновения исключений, сбоев и событий, связанных с информационной безопасностью.

Рекомендации по применению

Записи о событиях должны включать, насколько применимо:

a) идентификатор пользователя;

b) действия в системе;

c) даты, время и детали ключевых событий, например, входа в систему и выхода из нее;

d) обозначение устройства или размещение, если есть такая возможность, а также системный идентификатор;

e) записи успешных и отклоненных системой попыток доступа;

f) записи успешных и отклоненных системой попыток доступа к данным и иным ресурсам;

g) изменения в системной конфигурации;

h) использование привилегий;

i) использование системных утилит и приложений;

j) файлы, к которым осуществлялся доступ и вид доступа;

k) сетевые адреса и протоколы;

l) предупреждения, выданные системой контроля доступа;

m) активация и деактивация систем защиты, таких как антивирусы и системы обнаружения проникновения;

n) записи транзакций, выполненных пользователем в приложениях.

Регистрация событий служит источником данных для автоматизированных систем мониторинга, которые способны генерировать консолидированные отчеты и предупреждения системы безопасности.

Дополнительная информация

Журналы могут содержать важные данные и персональную информацию. Должны быть предприняты соответствующие меры защиты конфиденциальности (см. 18.1.4).

Там, где это возможно, системные администраторы не должны иметь разрешения для стирания или отключения записи их собственных действий (см. 12.4.3).

12.4.2 Защита информации в журналах

Метод реализации

Средства для ведения журналов и внесенная в них информация должны быть защищены от несанкционированного вмешательства и несанкционированного доступа.

Рекомендации по применению

Меры защиты должны быть нацелены на предотвращение неавторизованных изменений информации в журналах и проблем функционирования устройств ведения журналов, включая:

a) изменение типов сообщений, которые были записаны;

b) удаление или редактирование лог-файлов;

c) недостаток необходимого свободного объема для записи на носителе, приводящего либо к сбою в записи события, либо перезаписи информации о предыдущих событиях.

Может потребоваться сохранять в архиве некоторые контрольные журналы в рамках политики сохранения записей или в силу наличия требования собирать и сохранять свидетельства (см. 16.1.7).

Дополнительная информация

Системные журналы часто содержат большой объем информации, значительная часть которой не связана с мониторингом информационной безопасности. Для выявления значимых с точки зрения мониторинга информационной безопасности события необходимо предусмотреть либо копирование записей соответствующего типа в другой журнал, либо использование подходящих системных утилит или инструментов аудита для контрольного считывания и удаления лишних записей из файла.

Системные журналы должны быть защищены, потому как если будет возможность изменять или удалять в них данные, то наличие таких измененных журналов может создавать ложное чувство безопасности. Для защиты журналов может применяться их копирование в режиме реального времени в систему, находящуюся вне контроля системного администратора или оператора.

12.4.3 Журналы действий администратора и оператора

Метод реализации

Должны быть зафиксированы действия системных администраторов и операторов, журналы должны быть защищены и регулярно просматриваться.

Рекомендации по применению

Пользователи, обладающие привилегированными учетными записями, могут иметь возможность манипулировать журналами устройств обработки информации, находящимися под их непосредственным управлением, следовательно, необходимо защитить и просматривать журналы для обеспечения контроля за привилегированными пользователями.

Дополнительная информация

Для контроля вмешательств системных и сетевых администраторов может применяться система обнаружения вмешательств, которая находится вне контроля системных и сетевых администраторов.

12.4.4 Синхронизация часов

Метод реализации

Время у всех информационных систем, обрабатывающих важную информацию, в пределах организации или домена безопасности должно быть синхронизировано с единым источником эталонного времени.

Рекомендации по применению

Должны быть документированы внутренние и внешние требования к представлению времени, синхронности и точности. Такие требования могут быть законодательными, нормативными, контрактными требованиями, стандартами соответствия или требованиями для внутреннего мониторинга. Должен быть определен стандартный эталон времени для применения в организации.

Дополнительная информация

Правильная установка компьютерных часов является важной для обеспечения точности контрольных записей, которые могут потребоваться в ходе расследования или как свидетельства в рамках судебного или дисциплинарного разбирательства. Неточные контрольные записи могут затруднять такие расследования и подрывать доверие к подобного рода свидетельствам. В качестве эталонного времени в системах регистрации могут быть использованы сигналы точного времени, передаваемые по радио и синхронизированные с национальным атомным эталоном времени. Для синхронизации всех серверов с эталонным временем может быть использован сетевой протокол синхронизации времени (NTP).

12.5 Контроль эксплуатируемого программного обеспечения

Задача: гарантировать целостность эксплуатируемых систем.

12.5.1 Установка программ в эксплуатируемых системах

Метод реализации

Должны быть внедрены процедуры для управления установкой программного обеспечения в эксплуатируемых системах.

Рекомендации по применению

Должны быть приняты во внимание следующие рекомендации по контролю изменений программного обеспечения в эксплуатируемых системах:

a) обновление эксплуатируемого программного обеспечения, приложений и программных библиотек должно выполняться только обученными администраторами при наличии соответствующего разрешения руководства (см. 9.4.5);

b) эксплуатируемые системы должны содержать только одобренный исполнимый код, но не отладочный код или компиляторы,

c) приложения и программное обеспечение операционной системы должны устанавливаться только после проведения тщательного и успешного тестирования; тесты должны охватывать такие области, как удобство применения, безопасность, влияние на другие системы и дружественность интерфейса и должны выполняться на отдельных системах (см. 12.1.4); при этом должно быть гарантировано, что все соответствующие исходные программные библиотеки были обновлены;

d) должна применяться система управления конфигурациями и системное документирование для сохранения контроля над всем устанавливаемым программным обеспечением;

e) должна быть разработана стратегия отката до того, как изменения будут внедрены;

f) должен вестись контрольный журнал всех обновлений рабочих программных библиотек;

g) должны сохраняться предыдущие версии приложений как мера страховки;

h) устаревшие версии программного обеспечения должны архивироваться вместе с необходимой информацией и переменными, процедурами, параметрами конфигурации и вспомогательными программами и храниться в архиве тот же срок, что и данные.

Поставляемое программное обеспечение, используемое в эксплуатируемых системах, должно быть обеспечено поддержкой на уровне производителя. Спустя какое-то время

продавцы программного обеспечения прекратят поддержку устаревших версий. Организация должна принимать во внимание риски, связанные с этим обстоятельством.

Любое решение об обновлении до новой версии должно основываться на требованиях изменений, исходящих от бизнеса, и защищенности новой версии, например, введении новой функциональности, связанной с информационной безопасностью, или количестве и серьезности проблем информационной безопасности, влияющих на эту версию. Патчи к программному обеспечению должны устанавливаться в тех случаях, когда они могут помочь устранить или уменьшить уязвимости в информационной безопасности (см. 12.6).

Любой вид доступа поставщикам в целях обеспечения поддержки должен даваться только тогда, когда это необходимо, и с разрешения руководства. Действия поставщиков должны контролироваться (см. 15.2.1).

Компьютерное программное обеспечение может зависеть от извне поставляемых программ и модулей, которые должны контролироваться во избежание неавторизованных изменений, способных породить уязвимости в защите.

12.6 Управление техническими уязвимостями

Задача: предотвратить использование технических уязвимостей.

12.6.1 Управление техническими уязвимостями

Метод реализации

Должна своевременно получаться информация о технических уязвимостях в используемых информационных системах, должно оцениваться влияние этих уязвимостей на организацию и приниматься соответствующие меры для обработки связанных с этих рисков.

Рекомендации по применению

Ведение актуального и полного учета активов (см. раздел 8) – это необходимое условие для результативного управления техническими уязвимостями. Информация, необходимая для поддержки управления техническими уязвимостями, включает в себя наименование поставщика программного обеспечения, номер версии, текущее состояние (например, какое программное обеспечение установлено на какой системе) и лиц, ответственных в организации за это программное обеспечение.

Должны предприниматься соответствующие и своевременные действия в случае выявления потенциальных технических уязвимостей. Необходимо выполнять следующие рекомендации для разработки результативного процесса управления техническими уязвимостями:

a) организация должна определить и установить должности и обязанности, связанные с управлением техническими уязвимостями, включая мониторинг, оценку рисков, исправление, отслеживание активов и любые необходимые обязанности по координации;

b) для программного обеспечения и других технических систем (включенных в реестр активов, см. 8.1.1) должны быть определены информационные ресурсы, которые будут использованы для выявления существенных технических уязвимостей и поддержки осведомленности о них; эти информационные ресурсы должны обновляться в соответствии с изменениями в реестре или когда обнаруживаются другие новые или полезные ресурсы;

c) должен быть определен срок реагирования на уведомление о возможных существенных технических уязвимостях;

d) как только выявлена техническая уязвимость, организация должна определить

связанные с ней риски и необходимые действия; такого рода действия могут включать в себя выпуск патчей для устранения уязвимостей в системе или применение иных мер;

e) в зависимости от срочности устранения технической уязвимости, действия должны предприниматься или в соответствии с процедурами управления изменениями (см. 12.1.2), либо в соответствии с процедурами обработки инцидентов информационной безопасности (см. 16.1.5);

f) если патч доступен на легальном источнике, то должны быть оценены риски, связанные с установкой патча (риски, вызываемые уязвимостью, необходимо сравнить с рисками установки патча);

g) патчи должны быть протестированы и оценены до их установки для гарантии того, что они результативны и не приводят к недопустимым побочным эффектам; если нет доступного патча, необходимо рассмотреть возможность применения иных мер, таких как:

   1) прекращение пользование сервисами и инструментами, связанными с уязвимостями;

   2) настройка или добавление средств контроля доступа, например, брандмауэров, на стыке сетей (см. 13.1);

   3) ужесточение мониторинга для выявления реальных атак;

   4) дополнительное информирование о уязвимости;

h) для всех предпринятых действий должны сохраняться контрольные журналы;

i) процесс управления техническими уязвимостями должен регулярно контролироваться и оцениваться с тем, чтобы гарантировать его результативность и эффективность;

j) системы с высоким уровнем риска должны рассматриваться в первую очередь;

k) результативный процесс управления техническими уязвимостями должен быть увязан с деятельностью по управлению инцидентами, чтобы передавать данные об уязвимостях службе обработки инцидентов и обеспечивать техническими процедурами, которые должны быть выполнены, если произойдет инцидент;

l) определить процедуры обработки ситуации, когда уязвимость уже выявлена, но нет соответствующих контрмер. В такой ситуации организации должна оценить риски, связанные с известной уязвимостью и определить соответствующие действия по обнаружению и корректирующие действия.

Дополнительная информация

Управление техническими уязвимостями может рассматриваться как подфункция управления изменениями и, таким образом, может использовать процессы и процедуры управления изменениями (см. 12.1.2 и 14.2.2).

Производители часто находятся под значительным давлением необходимости выпустить патчи как можно быстрее. Вследствие чего существует возможность того, что патч не устраняет проблему надлежащим образом и имеет негативные побочные эффекты. Также в некоторых случаях деинсталляция патча после его применения не может быть выполнена достаточно легко.

Если соответствующее тестирование патча невозможно, например, в силу высокой стоимости или нехватки ресурсов, то может быть рассмотрена возможность задержки его применения для оценки соответствующих рисков, основанной на отчетах по применению патча другими пользователями. Может быть полезно использование стандарта ISO/IEC 27031 [14].

12.6.2 Ограничения на установку программного обеспечения

Метод реализации

Правила, регулирующие установку программного обеспечения пользователями, должны быть разработаны и внедрены.

Рекомендации по применению

Организация должна определить и следовать жесткой политике, определяющей, какое программное обеспечение пользователи могут устанавливать.

Необходимо исходить из принципа минимальных привилегий. Пользователи могут иметь возможность установки программного обеспечения, если только им даны такие полномочия. Организация должна определить, какого рода установки разрешены (например, обновления или патчи по безопасности существующего программного обеспечения), а также какие виды установок запрещены (например, программы для личного пользования или программы, происхождение которых, с учетом потенциальной вредоносности, неизвестно или подозрительно). Рассматриваемые полномочия должны даваться с учетом роли пользователя.

Дополнительная информация

Неконтролируемые установки программного обеспечения на компьютерах могут вести к появлению уязвимостей и, тем самым, к утечке информации, потере целостности или иным инцидентам информационной безопасности, либо к нарушению авторских прав.

12.7 Ограничения на аудит информационных систем

Задача: минимизировать воздействие аудита на эксплуатируемые системы.

12.7.1 Средства управления аудитом информационных систем

Метод реализации

Требования и действия по аудиту, направленному на проверку эксплуатируемых систем, должны тщательно планироваться и согласовываться с целью минимизации нарушений нормального выполнения бизнес-процессов.

Рекомендации по применению

Необходимо иметь в виду следующие рекомендации:

a) при аудите требования по доступу к системам и данным должны быть согласованы с соответствующим руководством;

b) область применения тестов технического аудита должна быть согласована и контролироваться;

c) проверочные тесты должны быть ограничены доступом к программному обеспечению и данным только на чтение;

d) доступ, отличный от режима только на чтение, должен быть разрешен только для изолированных копий системных файлов, которые должны быть удалены после завершения аудита или соответствующим образом защищены, если есть обязательства сохранять их в силу требований по документированию аудита;

e) требования к специальной или дополнительной обработке должны быть установлены и согласованы;

f) проверочные тесты, которые могут влиять на возможности системы, должны запускаться во внеурочное время;

g) любой доступ должен контролироваться и регистрироваться для обеспечения возможности прослеживания.

13 Безопасность обмена информацией

13.1 Управление сетевой безопасностью

Задача: гарантировать защиту информации в сетях и на поддерживающих их устройствах обработки информации.

13.1.1 Средства управления сетями

Метод реализации

Сети должны управляться и контролироваться, чтобы защитить информацию в системах и приложениях.

Рекомендации по применению

Должны быть внедрены средства управления для гарантии безопасности информации в сетях и защиты подключенных сервисов от несанкционированного доступа. В частности, следует принять во внимание следующее:

a) должны быть установлены обязанности и процедуры для управления сетевым оборудованием;

b) там, где это применимо, ответственность, связанная с эксплуатацией сетей, должна быть отделена от эксплуатации компьютеров (см. 6.1.2);

c) должны быть предприняты специальные меры для защиты конфиденциальности и целостности данных, передаваемых по сетям общего пользования или беспроводным сетям, а также подключенных систем и приложений (см. раздел 10 и 13.2); специальные меры могут также потребоваться для поддержания готовности сетевых сервисов и подключенных компьютеров;

d) должна вестись соответствующая регистрация и контроль с целью фиксации и выявления действий, которые могут повлиять на информационную безопасность или являются важными для нее;

e) действия по управлению должны тесно координироваться как для того, чтобы оптимизировать обслуживание организации, так и для гарантии того, что средства управления применяются согласованно в рамках инфраструктуры обработки информации;

f) системы в сетях должны быть прошедшими процедуру аутентификации;

g) системные соединения в сети должны быть ограничены.

Дополнительная информация

Дополнительная информация по сетевой безопасности может быть найдена в стандарте ISO/IEC 27033 [15][16][17][18][19].

13.1.2 Безопасность сетевых сервисов

Метод реализации

Должны быть определены для всех сетевых услуг и включены в соглашения по обслуживанию сетей механизмы обеспечения безопасности, уровни сервиса и требования к управлению, осуществляются ли эти услуги внутренними подразделениями или сторонней организацией.

Рекомендации по применению

Должна быть определена и регулярно проверяться способность провайдера сетевых услуг управлять согласованными услугами, обеспечивая безопасность, а также должно быть

согласовано право на аудит.

Должны быть определены меры по обеспечению безопасности, необходимые для конкретных услуг, такие как средства безопасности, уровень обслуживания и требования к управлению. Организация должна гарантировать, что провайдеры сетевых услуг осуществляют эти меры.

Дополнительная информация

Сетевые услуги включают в себя обеспечение подключения, услуги частных сетей (VPN), сетей с расширенными возможностями (VAN), а также решения по сетевой безопасности с возможностью управления, такие как брандмауэры и системы обнаружения проникновения. Эти услуги могут варьироваться в диапазоне от простого предоставления полосы пропускания до сложных предложений, расширяющих возможности.

Особенностями в обеспечении безопасности сетевых услуг могут быть:

a) совокупность методов, применяемых для защиты сетевых услуг, таких как аутентификация, шифрование и контроль сетевых соединений;

b) технические параметры, требуемые для защищенных соединений с предоставляемыми по услуге сетями в соответствии с правилами сетевых соединений;

c) процедуры использования сетевых услуг с целью ограничения доступа к предоставляемым сетям или приложениям, если необходимо.

13.1.3 Разделение в сетях

Метод реализации

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

Рекомендации по применению

Один из методов управления большими сетями состоит в разделении их на отдельные сетевые домены.

Домены могут быть выделены по уровню доверия (например, домен общего доступа, домен рабочих станций, домен сервера), по подразделениям (например, отдел кадров, финансовый, маркетинга) или по совокупности признаков (например, домен сервера, соединенный с множеством структурных подразделений). Разделение может быть осуществлено либо физическим разделением на разные сети, либо логическим (например, виртуальные частные сети, VPN).

Границы каждого домена должны быть четко определены. Обмен между доменами разрешен, но должен быть контролируемым на границе с использованием шлюзов (например, брандмауэров, фильтрующих маршрутизаторов). Критерии деления сетей на домены и разрешения доступа через шлюзы должны базироваться на оценке требований по безопасности каждого домена. Оценка должна производиться в соответствии с политикой контроля доступа (см. 9.1.1), требований к доступу, значимости и категории обрабатываемой информации, а также с учетом относительной стоимости и влияния применяемых технологий шлюзов на производительность.

Беспроводные сети требуют специальных решений в силу того, что в них сложно определить границы. В отношении критически важных сегментов следует принять подход, при котором все запросы из беспроводных сетей рассматриваются как внешние и отличаются от запросов внутренних сетей до тех пор, пока запрос не пройдет шлюз и не будет разрешен доступ к внутренним системам в соответствии с политикой сетевого контроля (см. 13.1.1).

Аутентификации, шифрования и технологий контроля доступа на уровне пользователя

современных беспроводных сетей, основанных на стандартах, может быть достаточно для прямого соединения к внутренней сети организации при надлежащем исполнении.

Дополнительная информация

Сети часто выходят за границы организации, поскольку деловое сотрудничество требует взаимодействия и совместного использования сетевого оборудования и устройств обработки информации. Такое расширение может увеличивать риск неавторизованного доступа к информационным системам организации, использующим сеть, некоторые из которых требуют защиты от пользователей других сетей в силу их критической важности или уязвимости.

13.2 Передача информации

Задача: обеспечить безопасность информации, передаваемой внутри организации и за ее пределы.

13.2.1 Политики и процедуры передачи информации

Метод реализации

Должны быть разработаны политики, процедуры и средства управления для защиты передачи информации, осуществляемой посредством любых типов коммуникационного оборудования.

Рекомендации по применению

Процедуры и средства управления, которым необходимо следовать при использовании коммуникационного оборудования для передачи информации, должны предусматривать следующее:

a) процедуры, предназначенные для защиты передаваемой информации от перехвата, копирования, изменения, перенаправления и разрушения;

b) процедуры для обнаружения вредоносного кода, который может передаваться средствами электронной коммуникации, и защиты от него;

c) процедуры для защиты конфиденциальной информации в электронном виде, передаваемой в форме приложения;

d) политику или руководящие указания, определяющие допустимое применение коммуникационных устройств (см. 8.1.3);

e) обязанности персонала, внешних сторон и любых иных пользователей не предпринимать действий, компрометирующих организацию, например, посредством клеветы, оскорблений, неправомерного представления себя от лица организации, рассылки писем по цепочке, неавторизованных закупок и т.д.;

f) использование криптографических средств, например, для защиты конфиденциальности, целостности и достоверности информации (см. раздел 10);

g) рекомендации по срокам хранения и утилизации всей деловой переписки, включая сообщения, соответствующие национальному и местному законодательству и нормативным документам;

h) средства управления и ограничения, связанные с использованием коммуникационных устройств, например, автоматическое перенаправление электронной почты на внешние адреса;

i) рекомендации персоналу предпринимать меры предосторожности, чтобы не раскрыть конфиденциальную информацию;

j) не оставлять сообщения, содержащие конфиденциальную информацию на

автоответчиках, т.к. они могут быть прослушаны неавторизованными лицами, сохранены в системах общего пользования или записаны не на том устройстве в результате ошибочного набора номера;

k) информирование персонала о проблемах, связанных с использованием факсов и соответствующих услуг, а именно:
   1) неавторизованным доступом к записям сообщений и их прослушиванием;
   2) преднамеренным или случайным программированием факса на отправку сообщений на определенные номера;
   3) отсылкой документов и сообщений на неверный номер либо в результате ошибочного набора, либо вызова сохраненного неверного номера.

Кроме того, персонал должен помнить, что не следует вести конфиденциальных разговоров в общественных местах или по небезопасным каналам связи, в открытых офисах и комнатах для переговоров.

Услуги по передачи информации должны соответствовать всем законодательным требованиям (см. 18.1).

Дополнительная информация

Передача информации может осуществляться посредством использования ряда различных средств связи, включая электронную почту, голосовую и факсимильную связь, а также видео.

Передача программ может осуществляться с помощью различных носителей, включая загрузку из Интернета и получение от поставщика, продающего готовые продукты.

Должны быть учтены юридические последствия, влияние на бизнес и безопасность, связанные с обменом электронными данными, электронной торговлей и электронными коммуникациями, а также требованиями к средствам управления.

13.2.2 Соглашения по передаче информации

Метод реализации

Соглашения должны регламентировать безопасную передачу бизнес-информации между организацией и внешними сторонами.

Рекомендации по применению

Соглашения по передаче информации должны включать следующее:

a) обязанности руководства по контролю и уведомлению о передаче, отправке и получению;
b) процедуры для обеспечения прослеживаемости и неопровержимости авторства;
c) минимальные технические стандарты для пакетирования и передачи;
d) соглашения об условном депонировании;
e) стандарты по идентификации курьеров;
f) ответственность и обязательства в случае инцидентов информационной безопасности, таких как потеря данных;
g) использование согласованной системы маркирования уязвимой и критически важной информации, гарантирующей, что смысл маркировки понятен сразу и что информация надлежащим образом защищена (см 8.2);
h) технические стандарты для записи и чтения информации и программного обеспечения;
i) любые специальные меры защиты, которые требуются для защиты уязвимых

элементов, такие как криптография (см. раздел 10);

j) цепочку ответственности и сохранности информации в процессе передачи;

k) приемлемые уровни контроля доступа.

Должны быть разработаны и поддерживаться политики, процедуры и стандарты по защите информации и физических носителей в процессе передачи (см 8.3.3), а также они должны быть указаны в соглашениях о передаче.

Часть любого соглашения, посвященная информационной безопасности, должна отражать степень конфиденциальности бизнес-информации, участвующей в передаче.

Дополнительная информация

Соглашения могут быть в электронном виде или рукописном, или же иметь форму официального договора. В отношении конфиденциальной информации конкретные механизмы, используемые для передачи такой информации, должны быть едиными для всех организаций и типов соглашений.

13.2.3 Электронные сообщения

Метод реализации

Информация, передаваемая электронными сообщениями, должна быть соответствующим образом защищена.

Рекомендации по применению

Рекомендации по информационной безопасности электронных сообщений должны включать следующее:

a) соответствующую схеме классификации, принятой организацией, защиту сообщений от несанкционированного доступа, изменения или отказа в обслуживании;

b) обеспечение правильной адресации и передачи сообщения;

c) надежность и доступность услуги;

d) правовые аспекты, например, требования к электронным подписям;

e) получение одобрения до использования внешних общественных сервисов, таких как служба мгновенных сообщений, социальные сети или файлообменник;

f) более высокий уровень аутентификации при контроле доступа из общедоступных сетей.

Дополнительная информация

Существует много видов электронных сообщений, таких как электронная почта, обмен электронными данными и социальные сети, которые играют определенную роль в бизнес-коммуникациях.

13.2.4 Соглашения о конфиденциальности или неразглашении

Метод реализации

Требования к соглашениям о конфиденциальности или неразглашении, отражающие потребности организации в защите информации, должны быть определены, документированы и регулярно пересматриваться.

Рекомендации по применению

Соглашения о конфиденциальности или неразглашении должны устанавливать требования по защите конфиденциальной информации в юридически обязывающей форме. Соглашения о конфиденциальности или неразглашении применимы к внешним сторонам или работникам организации. Содержание должно определяться в зависимости от типа стороны, принимающей обязательства, и ее прав доступа или обработки конфиденциальной

информации. Для определения требований к соглашениям о конфиденциальности или неразглашении должно быть принято во внимание следующее:

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

b) ожидаемый срок действия соглашения, включая случаи, когда конфиденциальность должна обеспечиваться в течение неопределенного времени;

c) действия, необходимые при расторжении соглашения;

d) обязанности и действия подписавших соглашение для избежания несанкционированного разглашения информации;

e) владение информацией, коммерческими секретами и интеллектуальной собственностью и как это связано с защитой конфиденциальной информации;

f) разрешенное использование конфиденциальной информации и права подписавшего на использование информации;

g) права на контроль деятельности, связанной с конфиденциальной информацией;

h) процесс уведомления и отчета о несанкционированном разглашении или утечке конфиденциальной информации;

i) сроки, в которые информация должна быть возвращена или уничтожена в случае прекращения действия соглашения;

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

В зависимости от требований организации к информационной безопасности может потребоваться отразить в соглашении о конфиденциальности и неразглашении и другие аспекты.

Соглашения о конфиденциальности и неразглашении должны соответствовать действующему законодательству и нормативным документам в той юрисдикции, в которой они применяются (см. 18.1).

Требования к соглашениям о конфиденциальности и неразглашении должны пересматриваться периодически и в том случае, когда происходят изменения, затрагивающие эти требования.

Дополнительная информация

Соглашения о конфиденциальности и неразглашении защищают информацию организации и доводят до сведения подписавших их обязанности по защите, использованию и разглашению информации в духе ответственности и полномочий.

Организации может потребоваться использовать различные формы соглашений о конфиденциальности и неразглашении в зависимости от обстоятельств.

14 Приобретение, разработка и обслуживание систем

14.1 Требования по безопасности информационных систем

Задача: гарантировать, что информационная безопасность является неотъемлемой частью информационных систем в течение всего их жизненного цикла. Это также относится и к требованиям для информационных систем, которые предоставляют сервисы в общедоступных сетях.

14.1.1 Анализ и установление требований по информационной безопасности

Метод реализации

Требования, связанные с информационной безопасностью, должны быть включены в требования для новых информационных систем или расширения к существующим информационным системам.

Рекомендации по применению

Требования по информационной безопасности должны быть определены, используя различные методы, такие как выделение требований по соответствию из политик и регламентов, моделирование угроз, анализ инцидентов или использование порогов уязвимости. Результаты определения должны быть документированы и рассмотрены всеми заинтересованными сторонами.

Требования по информационной безопасности и средства управления должны отражать ценность защищаемой информации для бизнеса (см. 8.2) и потенциальное негативное влияние на бизнес, которое может быть следствием недостаточно надежной защиты.

Определение и управление требованиями по информационной безопасности и соответствующими процессами должны быть объединены на ранних стадиях проектов информационных систем. Раннее внимание к требованиям по информационной безопасности, например, на стадии проектирования, может приводить к более результативным и экономически эффективным решениям.

Требования по информационной безопасности должны также учитывать:

a) уровень надежности, необходимый для требуемой идентификационной информации пользователей, чтобы установить требования к аутентификации пользователей;

b) процессы обеспечения доступа и авторизации как для обычных пользователей, так и для привилегированных или технических специалистов;

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

d) потребности, связанные с требуемой защитой используемых активов, в особенности, относящиеся к готовности, конфиденциальности и целостности;

e) требования, вытекаемые из бизнес-процессов, такие как контроль и регистрация транзакций, требования по неопровержимости авторства;

f) требования, устанавливаемые другими средствами обеспечения защиты, например, средствами взаимодействия с системами регистрации и мониторинга или обнаружения утечки данных.

Для приложений, которые обеспечивают сервисы в общественных сетях или осуществляют транзакции, должны быть приняты во внимание специальные средства, указанные в п. 14.1.2 и 14.1.3.

Для приобретаемых продуктов процесс тестирования и закупки должен быть следующим. Контракты с поставщиком должны содержать установленные требования по безопасности. В тех случаях, когда функциональность предлагаемых продуктов, связанная с защитой, не удовлетворяет установленным требованиям, должны быть пересмотрены риски и средства управления до покупки продукта.

Должно быть изучено и выполнено имеющееся руководство по настройке защиты продукта, соответствующее последнему составу программ/служб системы.

Критерии принятия продуктов должны быть определены, например, с точки зрения их функциональности, которая гарантирует, что установленные требования по защите будут выполнены. Продукты должны быть оценены по этим критериям до приобретения.

Дополнительная функциональность должна быть проанализирована, чтобы гарантировать, что она не несет каких-либо дополнительных неприемлемых рисков.

Дополнительная информация

ISO/IEC 27005 [11] и ISO 31000 [27] содержат руководство по применению процессов менеджмента риска к определению средств управления для выполнения требований по информационной безопасности.

14.1.2 Защита прикладных услуг в сетях общего пользования

Метод реализации

Информация, используемая прикладными услугами, передающаяся по общедоступным сетям, должна быть защищена от мошеннических действий, претензий, связанных с нарушениями контрактных обязательств, и несанкционированного раскрытия и изменения.

Рекомендации по применению

Факторы, учитываемые при защите информации, используемой прикладными услугами, передающейся по общедоступным сетям, должны включать следующее:

a) уровень надежности, который каждая сторона требует от предъявляемой другой стороной идентификационной информации, например, посредством аутентификации;
b) процессы санкционирования, связанные с лицами, которые могут одобрить содержание, выпуск или подписать ключевые деловые документы;
c) гарантию того, что партнеры по обмену информацией полностью информированы об их правах по предоставлению и использованию услуг;
d) определение и выполнение требований по конфиденциальности, целостности, подтверждению отправки и получения ключевых документов, а также по неопровержимости авторства контрактов, например, связанных с тендерными или договорными процессами;
e) уровень доверия, необходимый для уверенности в целостности ключевых документов;
f) требования по защите любой конфиденциальной информации;
g) конфиденциальность и целостность любой передачи данных по заказам, платежам, адресам поставки и подтверждению получения;
h) уровень проверки, обеспечивающий подтверждение платежной информации, предоставляемой заказчиком;
i) выбор наиболее подходящих форм расчетов для защиты от мошенничества;
j) уровень защиты, требуемый для обеспечения конфиденциальности и целостности информации по заказу;
k) избежание потерь или дублирования информации по операциям;
l) ответственность, связанную с мошенническими операциями;
m) требования по страхованию.

Многие рекомендации из перечисленных выше могут быть выполнены применением криптографических методов (см. раздел 10), с учетом соответствия требованиям законодательства (см. раздел 18, особенно 18.1.5 для законодательства в области криптографии).

Отношения в сфере прикладных услуг между партнерами должны поддерживаться документированным соглашением, которое устанавливает обязательства обеих сторон по согласованным условиям применения услуг, включая детали авторизации (см п. «b» выше).

Должны быть приняты во внимание требования устойчивости к атакам, которые могут включать требования по защите используемых серверов приложений, или гарантию доступности межсетевых соединений, требуемых для выполнения услуг.

Дополнительная информация

Приложения, доступные через сети общего пользования, подвержены ряду угроз, таких как мошенническая деятельность, нарушение условий договора или публичное раскрытие информации. Поэтому обязательны детальная оценка рисков и соответствующий выбор средств управления. Требуемые средства управления часто включают в себя криптографические методы для аутентификации и безопасной передачи данных.

Прикладные услуги могут использовать безопасные аутентификационные методы, например, применение криптографии с открытым ключом или цифровых подписей (см. раздел 10), для снижения рисков. Также могут быть задействованы доверенные третьи стороны там, где такие услуги необходимы.

14.1.3 Защита операций прикладных услуг

Метод реализации

Информация, участвующая в операциях, осуществляемых при пользовании прикладными услугами, должна быть защищена с целью предотвращения незавершенной передачи, неправильной маршрутизации, несанкционированного изменения сообщения, несанкционированного раскрытия, несанкционированного дублирования сообщения или воспроизведения.

Рекомендации по применению

Факторы, учитываемые при защите операций, осуществляемых при пользовании прикладными услугами, должны включать следующее:

a) использование электронных подписей каждой стороной, участвующей в операции;
b) все аспекты операции, т.е. обеспечение того, что
    1) секретная информация для аутентификации пользователей является проверенной и действующей;
    2) операция остается конфиденциальной;
    3) сохраняется конфиденциальность для всех участвующих сторон;
c) каналы связи между участвующими сторонами являются шифрованными;
d) протоколы для обмена данными между участвующими сторонами являются защищенными;
e) гарантию того, что хранение подробностей операции осуществляется за пределами общедоступной зоны, например, на платформах хранения, существующих во внутренней сети организации, и эта информация не сохраняется и не копируется на носители, непосредственно доступные из Интернета;
f) в тех случаях, когда используется доверенный центр сертификации (например, в целях выпуска и поддержки цифровых подписей или цифровых сертификатов) защита является комплексной и встроена в сквозной процесс управления подписями/сертификатами.

Дополнительная информация

Степень выбранного контроля должна быть соизмерима с уровнем риска, связанного с каждой конкретной формой операции прикладной услуги.

Для операций может требоваться соответствие законодательным и нормативным требованиям в рамках той юрисдикции, где операция генерируется, совершается, завершается и сохраняется.

14.2 Безопасность в процессах разработки и поддержки

Задача: гарантировать, что меры по обеспечению информационной безопасности разработаны и реализуются в течение всего цикла разработки информационных систем.

14.2.1 Политика безопасности при разработке

Метод реализации

Правила для разработки программного обеспечения и систем должны быть установлены и применяться ко всем разработкам в организации.

Рекомендации по применению

Безопасная разработка является требованием при построении защищенных сервисов, архитектуры, программного обеспечения и систем. В рамках политики безопасной разработки должны быть учтены следующие аспекты:

a) безопасная среда разработки;
b) руководящие указания по обеспечению безопасности в течение жизненного цикла разработки:
    1) безопасная методология разработки программного обеспечения;
    2) руководство по безопасному кодированию для каждого используемого языка программирования;
c) требования по безопасности на стадии проектирования;
d) контрольные точки проверки безопасности в рамках этапов проекта;
e) защищенные репозитории;
f) безопасность при управлении версиями;
g) требуемые знания о безопасности приложений;
h) способность разработчиков избегать, обнаруживать и устранять уязвимости.

Должны использоваться безопасные методы программирования как для новых разработок, так и для кодирования повторно используемых фрагментов, для которых неизвестны использованные при их разработке стандарты или же они несовместимы с текущей практикой. Должны быть предусмотрены стандарты безопасного кодирования и, где это важно, они должны быть обязательными. Разработчики должны быть обучены применению этих стандартов и тестированию, а анализ кода должен служить проверкой их применения.

Если разработка отдана на аутсорсинг, организация должна получить гарантии, что внешняя сторона соответствует вышеприведенным правилам безопасной разработки (см. 14.2.7).

Дополнительная информация

Разработка может вестись средствами самих приложений, таких как офисные пакеты, скриптовые языки, браузеры или базы данных.

14.2.2 Процедуры управления системными изменениями

Метод реализации

Изменения в системах в течение цикла разработки должны быть управляемыми посредством формализованных процедур управления изменениями.

Рекомендации по применению

Должны быть документированы и выполняться процедуры управления изменениями, чтобы гарантировать целостность системы, приложений и продуктов, от ранних стадий

проектирования до всех последующих действий по поддержке.

Внедрение новых систем и крупных изменений в существующие системы должно происходить в соответствии с формализованным процессом документирования, спецификации, тестирования, контроля качества и управляемой реализации.

Этот процесс должен включать в себя оценку риска, анализ влияния изменений и определение необходимых средств управления безопасностью. Этот процесс также должен гарантировать, что существующие процедуры защиты и управления не нарушены, что программисты, осуществляющие поддержку, имеют доступ только к той части системы, которая необходима для их работы и что официальное согласование и одобрение для любых изменений получены.

Там, где это возможно, процедуры управления изменениями для приложений и операционной среды должны быть объединены (см. 12.1.2). Процедуры управления изменениями должны включать, но не ограничиваться, следующее:

a) ведение записей о согласованных уровнях авторизации;
b) гарантию того, что изменения подтверждены авторизованными пользователями;
c) анализ средств управления и целостности процедур, чтобы гарантировать, что они не будут нарушены изменениями;
d) выявление программного обеспечения, информации, элементов баз данных и оборудования, которые требуют изменений;
e) выявление и проверка критического с точки зрения безопасности кода для минимизации вероятности реализации известных угроз безопасности;
f) получение формального одобрения детализированных предложений до начала работы;
g) гарантию, что изменения одобрены до их реализации авторизованными пользователями;
h) гарантию того, что комплект системной документации обновлен по завершении каждого изменения и что предыдущие версии документов помещены в архив или уничтожены;
i) поддержку контроля версий для всех изменений программного обеспечения;
j) ведение контрольных записей по всем запросам на изменения;
k) гарантию того, что рабочая документация (см. 12.1.1) и пользовательские процедуры изменены таким образом, чтобы остаться соответствующими;
l) гарантирование того, что осуществление изменений производится в надлежащий момент времени и не препятствует выполнению затрагиваемых бизнес-процессов.

Дополнительная информация

Изменение программного обеспечения может влиять на операционную среду и наоборот.

Хорошая практика подразумевает тестирование нового программного обеспечения в среде, отделенной как от среды разработки, так и от рабочей среды (см. 12.1.4). Это обеспечивает механизмы контроля нового программного обеспечения и возможность дополнительной защиты рабочей информации, которая используется для целей тестирования. Это также относится к патчам, сервис-пакам и другим обновлениям.

Там, где предполагается автоматическое обновление, должен быть оценен риск для целостности и готовности системы в сравнении с выигрышем в скорости развертывания обновления. Не должно использоваться автоматическое обновление для критических систем, так как некоторые обновления могут вызывать падение критических приложений.

14.2.3 Технический анализ приложений после изменения операционной платформы

Метод реализации

После изменения операционных платформ, критичные бизнес-приложения должны быть проанализированы и протестированы, чтобы гарантировать, что отсутствует негативное влияние на деятельность организации или безопасность.

Рекомендации по применению

Этот процесс должен охватывать:

a) пересмотр процедур контроля и обеспечения целостности приложений для гарантии того, что они не были нарушены при изменениях операционных платформ;
b) гарантию того, что оповещение об изменениях операционной среды сделано своевременно, давая возможность провести соответствующие тесты и анализ до начала внедрения;
c) гарантию того, что сделаны соответствующие изменения в планах по непрерывности бизнеса (см. раздел 17).

Дополнительная информация

Операционные платформы включают в себя операционные системы, базы данных и промежуточное программное обеспечение. Должен также применяться контроль изменений приложений.

14.2.4 Ограничения на изменения в пакетах программ

Метод реализации

Модификация пакетов программ не должна поощряться и должна быть ограничена только необходимыми изменениями, а все изменения должны строго контролироваться.

Рекомендации по применению

Насколько это возможно и практически осуществимо, приобретаемое у поставщика программное обеспечение должно использоваться без изменений. В тех случаях, когда программный пакет требует изменений, должны приниматься во внимание следующие моменты:

a) риск нарушения встроенных средств управления и процессов обеспечения целостности;
b) должно ли быть получено согласие поставщика;
c) возможность получения требуемых изменений от поставщика как штатного обновления программы;
d) последствия того, что после внесения изменений организация станет ответственной за последующую поддержку программного обеспечения;
e) совместимость с другим используемым программным обеспечением.

Если изменения необходимы, то оригинал программного обеспечения должен остаться незатронутым, а изменения внесены в выделенную копию. Должен выполняться процесс управления обновлением программного обеспечения, чтобы гарантировать, что большинство актуальных согласованных патчей и обновлений приложений установлены для всего разрешенного к изменению программного обеспечения (см. 12.6.1). Все изменения должны быть полностью протестированы и документированы так, чтобы они могли быть произведены повторно, если необходимо, в ходе последующих обновлений программного обеспечения. Если требуется, то изменения должны быть протестированы и одобрены независимым испытательным центром.

14.2.5 Принципы разработки защищенных систем

Метод реализации

Принципы разработки защищенных систем должны быть установлены, документированы, поддерживаться и применяться во всех случаях внедрения информационных систем.

Рекомендации по применению

Должны быть разработаны, документированы и применяться в корпоративной деятельности по разработке информационных систем процедуры разработки защищенных информационных систем, основанные на принципах безопасной разработки. Защита должна быть встроена на всех архитектурных уровнях (бизнес, данные, приложения и технология), обеспечивая баланс между необходимостью защиты информации и требованиями к доступности. Новые технологии должны анализироваться в плане рисков для безопасности и проектные решения должны рассматриваться с точки зрения известных моделей атак.

Эти принципы и установленные процедуры разработки должны регулярно пересматриваться с тем, чтобы они способствовали результативному развитию стандартов безопасности в рамках процессов разработки. Они должны также регулярно пересматриваться для гарантии того, что они остаются актуальными в плане борьбы с любыми потенциальными новыми угрозами и пригодными в свете усовершенствований в используемых технологиях и решениях.

Установленные принципы безопасной разработки должны применяться, там, где это возможно, для информационных систем, переданных на аутсорсинг, через контракты и иные обязывающие соглашения между организацией и поставщиком. Организация должна подтверждать, что строгость принципов безопасной разработки поставщика сравнима с ее собственной.

Дополнительная информация

Процедуры разработки приложений должны использовать методы безопасного проектирования в разработке приложений, имеющих интерфейсы ввода-вывода. Методы безопасного проектирования обеспечивают методическую основу для методов авторизации пользователей, управления защитой сессии и подтверждения правильности данных, удаления отладочных кодов.

14.2.6 Безопасная среда разработки

Метод реализации

Организации должны обеспечивать и соответствующим образом защищать безопасные среды разработки и интеграции систем, охватывающие весь цикл разработки.

Рекомендации по применению

Безопасная среда разработки включает в себя персонал, процессы и технологии, связанные с разработкой и интеграцией систем.

Организация должна оценивать риски, связанные с определенными действиями по разработке систем, и формировать безопасные среды разработки для конкретных работ по разработке систем, принимая во внимание:

a) уязвимость данных, подлежащих обработке, хранению и передаче в системе;
b) действующие внешние и внутренние требования, например, регламенты или политики;
c) средства управления безопасностью, уже внедренные организацией для обеспечения разработки систем;

d) добросовестность персонала, работающего в данной среде (см. 7.1.1);

e) степень передачи на сторону работ, связанных с разработкой систем;

f) необходимость разделения различных сред разработки;

g) контроль доступа к среде разработки;

h) мониторинг изменений как самой среды разработки, так и кода, размещенного в ней;

i) резервные копии, сохраняемые на удаленных защищенных площадках;

j) контроль перемещения данных как в, так и из среды разработки.

Как только организация определила уровень защиты для конкретной среды разработки, она должна документировать соответствующие процессы в процедурах обеспечения безопасности разработки и обеспечить этими процедурами всех, кому они необходимы.

14.2.7 Разработка, переданная на аутсорсинг

Метод реализации

Организация должна контролировать и вести мониторинг процесса разработки системы, переданного на аутсорсинг.

Рекомендации по применению

Если разработка системы передана на аутсорсинг, для всех участников цепочки поставки организации должны учитываться следующие моменты:

a) лицензионные соглашения, права на код и интеллектуальную собственность, связанные с разрабатываемым на стороне контентом;

b) контрактные требования по безопасному проектированию, кодированию и тестированию (см. 14.2.1);

c) обеспечение внешнего поставщика утвержденной моделью угроз;

d) приемочное тестирование для обеспечения качества и корректности поставляемых продуктов;

e) обеспечение свидетельства того, что были применены пороговые критерии безопасности для установления минимально приемлемых уровней защищенности и конфиденциальности;

f) обеспечение свидетельства того, что было выполнено тестирование в достаточном объеме, чтобы подтвердить отсутствие преднамеренного или непреднамеренного вредоносного содержимого в поставляемых продуктах,

g) обеспечение свидетельства того, что было выполнено тестирование в достаточном объеме, чтобы подтвердить отсутствие известных уязвимостей,

h) соглашение об условном депонировании, если исходный код больше недоступен,

i) обусловленные контрактом права на аудит процессов разработки и средств управления ею

j) действующая документация на среду сборки, используемую для формирования поставляемых продуктов,

k) организация остается ответственной за соответствие действующему законодательству и проверку эффективности контроля.

Дополнительная информация

Дополнительная информация по взаимоотношениям с поставщиками может быть найдена в ISO/IEC 27036 [21][22][23].

14.2.8 Тестирование защищенности системы

Метод реализации

В ходе разработки должно выполняться тестирование функциональности, связанной с безопасностью.

Рекомендации по применению

Новые и обновляемые системы требуют тщательного тестирования и проверки в ходе процессов разработки, включая подготовку детального графика работ, исходных данных для тестирования и ожидаемых в некотором диапазоне условий результатов. При разработке собственными силами такие тесты должны первоначально выполняться командой разработки. Затем должно выполняться независимое приемочное тестирование (как для разработки собственными силами, так и для переданной на сторону), чтобы гарантировать, что система работает как ожидалось и только как ожидалось (см. 14.1.1 и 14.2.9). Объем тестирования должен соответствовать важности и характеру системы.

14.2.9 Приемочное тестирование системы

Метод реализации

Должно быть выбрано тестовое программное обеспечение и установлены критерии приемки для новых информационных систем, обновлений и новых версий.

Рекомендации по применению

Приемочное тестирование системы должно включать в себя проверку выполнения требований по информационной безопасности (см. 14.1.1 и 14.1.2) и соблюдения установленных правил безопасной разработки систем (см. 14.2.1). Тестирование должно проводиться также для полученных компонентов и встраиваемых систем. Организации могут применять автоматизированные средства, такие как анализаторы кода или сканеры уязвимостей, и должны проверять исправление связанных с безопасностью дефектов.

Тестирование должно выполняться в реалистичной тестовой среде, чтобы гарантировать, что проверяемая система не внесет уязвимостей в инфраструктуру организации и что результаты тестирования надежны.

14.3 Данные для тестирования

Задача: обеспечить защиту данных, используемых при тестировании.

14.3.1 Защита данных для тестирования

Метод реализации

Данные для тестирования должны тщательно выбираться, быть защищенными и контролироваться.

Рекомендации по применению

Следует избегать использования в целях тестирования информацию, содержащую личные данные человека, или какую-либо иную конфиденциальную информацию. Если же информация, содержащая личные данные человека, или какая-то другая конфиденциальная информация используется для целей тестирования, то все деликатные подробности и данные должны быть удалены или изменены (см. ISO/IEC 29101 [26]).

Для защиты рабочих данных, используемых в целях тестирования, рекомендуется применять следующие рекомендации:

а) процедуры контроля доступа, применяемые в действующих прикладных системах, следует также применяться и в системах тестирования приложений;

b) всякий раз, когда рабочая информация копируется в среду тестирования, следует применять отдельную авторизацию;

c) рабочая информация должна быть удалена из среды тестирования немедленно после того, как тестирование завершено;

d) копирование и использование рабочей информации должно регистрироваться, чтобы обеспечить возможность проверки.

Дополнительная информация

Системное и приемочное тестирование обычно требует значительных объемов тестовых данных, максимально близких к рабочим данным.

15 Отношения с поставщиками

15.1 Информационная безопасность в отношениях с поставщиками

Задача: гарантировать защиту активов организации, которые доступны поставщикам

15.1.1 Политика информационной безопасности в отношениях с поставщиками

Метод реализации

Требования по информационной безопасности для снижения рисков, связанных с доступом поставщиков к активам организации, должны быть согласованы с поставщиками и документированы.

Рекомендации по применению

Организация должна в политике определить и сделать обязательными средства управления информационной безопасностью, которые относятся именно к доступу поставщиков к информации организации. Эти средства управления должны определять процессы и процедуры, которые должны выполняться организацией, а также те процессы и процедуры, которые организация должна потребовать выполнять от поставщика, включая:

a) определение и документирование видов поставщиков, например, ИТ-услуги, услуги доставки, финансовых услуги, компоненты ИТ-инфраструктуры, которые будут иметь доступ к ее информации;

b) стандартизованный процесс и модель жизненного цикла для управления отношениями с поставщиками;

c) определение видов доступа к информации, которые будут разрешены для различных видов поставщиков, а также доступа с целью мониторинга и контроля;

d) минимальные требования по информационной безопасности для каждого вида информации и вид доступа для определения основных положений соглашения с конкретным поставщиком, учитывающих бизнес-потребности организации и требования, а также характер рисков;

e) процессы и процедуры для мониторинга соблюдения установленных требований по информационной безопасности для каждого вида поставщиков и вида доступа, включая проверку и валидацию продукции третьей стороной;

f) корректность и полноту средств управления для обеспечения целостности информации или обработки информации, проводимой любой из сторон;

g) виды обязательств, применимых к поставщикам для защиты информации организации;

h) обработку инцидентов и непредвиденных последствий, связанных с доступом поставщика, включая обязательства как организации, так и поставщика;

i) способность к восстановлению и, если необходимо, меры по восстановлению и аварийные меры для обеспечения доступности информации или обработки информации, предпринимаемые любой из сторон;

j) ознакомление персонала организации, участвующего в закупках, с действующими политиками, процессами и процедурами;

k) ознакомление персонала организации, взаимодействующего с персоналом поставщиков, с соответствующим правилами взаимодействия и поведения с учетом вида поставщика и уровня его доступа к системам организации и информации;

l) условия, при которых требования по информационной безопасности и средства управления будут включены в соглашение, подписанное обоими сторонами;

m) управление необходимой передачей информации, устройств обработки информации и чем-либо еще, нуждающимся в передаче, и гарантия того, что безопасность обеспечивается в течение всего периода передачи.

Дополнительная информация

При ненадлежащем управлении безопасностью могут возникать риски со стороны поставщиков. Должны быть определены и выполняться меры для управления доступом поставщиков к устройствам обработки информации. Например, если существует особая необходимость в сохранении конфиденциальности информации, может заключаться соглашение о неразглашении. Другой пример защиты данных от рисков, когда соглашение с поставщиками включает в себя вопросы передачи за границу или доступа к информации из-за границы. Организация должна помнить, что ответственность за соблюдение законодательства и контрактных обязательств лежит на самой организации.

15.1.2 Решение вопросов безопасности в соглашениях с поставщиками

Метод реализации

Все существенные требования по информационной безопасности должны быть установлены и согласованы с каждым поставщиком, который может получать доступ, обрабатывать, хранить, передавать информацию организации или поставлять компоненты для ИТ-инфраструктуры.

Рекомендации по применению

Соглашения с поставщиками должны быть разработаны и документированы с гарантией, что нет разногласий между организацией и поставщиком в отношении взаимных обязательств по выполнению соответствующих требований информационной безопасности.

Для выполнения установленных требований информационной безопасности следует рассмотреть с точки зрения включения в соглашения следующие положения:

a) определение предоставляемой информации или информации, к которой предоставляется доступ, а также методы предоставления информации или доступа к информации;

b) категории информации в соответствии со схемой классификации организации (см. 8.2); сопоставление, если необходимо, схем классификации организации и поставщика;

c) законодательные и нормативные требования, включая требования к защите данных, прав интеллектуальной собственности и авторских прав, а также описание того, каким образом будет гарантировано их выполнение;

d) обязательство каждой стороны контракта выполнять согласованный набор средств управления, включая контроль доступа, контроль выполняемых работ, мониторинг, отчетность и аудиты;

e) правила допустимого применения информации, включая описание недопустимого

использования, если необходимо;

f) либо полный перечень сотрудников поставщика, которым дан доступ к информации или право получать информацию от организации, или процедуры или условия для получения такого разрешения, а также аннулирования разрешения доступа или права получения информации организации персоналом поставщика;

g) политики информационной безопасности в соответствии с конкретным контрактом;

h) требования по управлению инцидентами и процедуры (особенно оповещения и совместной работы по устранению последствий инцидента);

i) ознакомление и обучение выполнению требований конкретных процедур и требований информационной безопасности, например, ответных действий по инциденту, процедур авторизации;

j) соответствующие регламенты для подрядчиков, включая средства управления, которые должны выполняться;

k) соответствующие контактные лица по соглашению, включая контактное лицо по вопросам информационной безопасности;

l) требования к предварительной проверке персонала поставщика, если таковые установлены, включая обязанности по проведению процедур предварительной проверки и информирования в случае, когда проверка не была завершена или ее результаты дают основания для сомнений или опасений;

m) право на аудит процессов поставщика и осуществление процедур контроля, связанных с контрактом;

n) процессы устранения дефектов и разрешения споров;

o) обязательство поставщика периодически предоставлять независимый отчет о результативности средств управления и согласие на своевременное решение соответствующих проблем, упомянутых в отчете;

p) обязательства поставщика соответствовать требованиям информационной безопасности организации.

Дополнительная информация

Соглашения могут существенно отличаться для различных организаций и различных видов поставщиков. В связи с этим следует уделить внимание тому, чтобы учесть все значимые риски, связанные с информационной безопасностью, и требования. Соглашения с поставщиками могут также допускать участие других сторон (например, субподрядчиков).

В соглашении должны быть предусмотрены процедуры обеспечения непрерывности производственных процессов, чтобы избежать любых задержек в замене продуктов и услуг в случае, если поставщик перестает быть способным поставлять эти продукты или услуги.

15.1.3 Цепочка поставок информационно-коммуникационных технологий

Метод реализации

Соглашения с поставщиками должны включать требования, учитывающие риски информационной безопасности, связанные с цепочкой поставок услуг и продуктов в сфере информационно-коммуникационных технологий.

Рекомендации по применению

В отношении безопасности цепочек поставок должны быть рассмотрены для включения в соглашения с поставщиками следующие положения:

a) определение требований информационной безопасности, применимых к закупкам

продуктов и услуг в сфере информационно-коммуникационных технологий, в дополнение к общим требованиям информационной безопасности, относящимся к взаимоотношениям с поставщиками;

b) требование для услуг в области информационно-коммуникационных технологий, чтобы поставщики распространяли требования организации, связанные с безопасностью, на всю цепочку поставки, если поставщик привлекает подрядчиков для выполнения какой-то части услуг в области информационно-коммуникационных технологий, оказываемых организации;

c) требование для продуктов в области информационно-коммуникационных технологий, чтобы поставщики распространяли соответствующие процедуры, связанные с безопасностью, на всю цепочку поставки, если эти продукты включают в себя компоненты, закупаемые у других поставщиков;

d) выполнение процесса мониторинга и подходящих методов для подтверждения, что поставляемые продукты и услуги в области информационно-коммуникационных технологий соответствуют установленным требованиям;

e) выполнение процесса определения компонентов продукта или услуги, которые важны для поддержки функциональности и, таким образом, требуют повышенного внимания и изучения, если созданы за пределами организации, особенно, если первичный поставщик передает на аутсорсинг производство каких-то элементов продукта или услуги другим поставщикам;

f) получение уверенности в том, что критически важные компоненты и их происхождение могут быть прослежены по всей цепочке поставки;

g) получение уверенности в том, что поставляемые в области информационно-коммуникационных технологий продукты и услуги функционируют ожидаемым образом и не имеют каких-либо непредусмотренных или нежелательных функций;

h) определение правил обмена информацией, касающихся цепочки поставки и любых возможных проблем и взаимных уступок между организацией и поставщиками;

i) выполнение конкретных процессов управления жизненным циклом компонентов информационно-коммуникационных технологий, а также доступностью и рисками, связанными с безопасностью. Это включает в себя управление рисками в отношении компонентов, которые более не доступны в силу того, что их поставщики прекратили свою деятельность, или прекратили поставку этих компонентов по причине развития технологий.

Дополнительная информация

Конкретные методы менеджмента риска в цепочке поставки информационно-коммуникационных технологий основаны на высокоуровневых процедурах обеспечения общей информационной безопасности, качества, управления проектами и разработки систем, но не заменяют их.

Организациям рекомендуется сотрудничать с поставщиками, чтобы иметь понимание всей цепочки поставки информационно-коммуникационных технологий и любых вопросов, которые оказывают значительное влияние на поставляемые продукты и услуги. Организации могут влиять на методы обеспечения информационной безопасности в цепочке поставок информационно-коммуникационных технологий четкой регламентацией в соглашениях со своими поставщиками вопросов, которые следует решить поставщикам по всей цепочке поставки информационно-коммуникационных технологий.

Цепочка поставки информационно-коммуникационных технологий, как она здесь понимается, включает в себя и услуги облачных технологий.

15.2 Управление предоставлением услуги поставщиком

Задача: поддерживать согласованный уровень информационной безопасности и предоставления услуги в соответствии с соглашениями с поставщиком

15.2.1 Мониторинг и анализ услуг поставщика

Метод реализации

Организациям следует регулярно отслеживать, анализировать и проводить аудит предоставления услуги поставщиком.

Рекомендации по применению

Мониторинг и анализ услуг поставщика должен гарантировать, что положения по информационной безопасности и условия соглашений выполняются и что инциденты и проблемы в области информационной безопасности решаются надлежащим образом.

Это должно реализовываться через процесс взаимодействия между организацией и поставщиком при управлении услугами, чтобы:

a) отслеживать уровень исполнения услуги для контроля соответствия соглашениям;

b) изучать отчеты об услуге, представляемые поставщиком, и организовывать регулярные рабочие совещания, как это определено соглашениями;

c) проводить аудиты поставщиков вместе с анализом отчетов независимых аудиторов, если они есть, и осуществлять последующие действия по выявленным проблемам;

d) получать информацию об инцидентах информационной безопасности и анализировать эту информацию, как требуется соглашениями, и любыми рабочими инструкциями и процедурами;

e) анализировать контрольные журналы поставщиков и записи о событиях информационной безопасности, эксплуатационных проблемах, сбоях, выявлении причин ошибок и нарушений, связанных с поставляемыми услугами;

f) разрешать любые выявленные проблемы;

g) анализировать взаимоотношения поставщика с его подрядчиками в части информационной безопасности;

h) гарантировать, что поставщик обеспечивает свою способность оказывать услуги на надлежащем уровне при наличии работоспособных планов, разработанных чтобы обеспечить согласованные уровни непрерывности оказания услуги при значительных сбоях и аварийных ситуациях в ходе оказания услуги (см. раздел 17).

Ответственность за управление взаимоотношениями с поставщиками должна быть возложена на выделенное лицо или группу по управлению услугами. Кроме того, организации следует гарантировать, что поставщикам установлена обязанность по анализу соответствия и обеспечению выполнения требований соглашения. Должны быть выделены достаточные ресурсы с необходимыми техническими навыками для мониторинга того, что требования соглашения, в частности, требования информационной безопасности, выполняются. Необходимо предпринять соответствующие действия при обнаружении недостатков в оказании услуг.

Организация должна сохранять достаточный общий контроль и осведомленность по всем аспектам безопасности в отношении уязвимой или критически важной информации или устройств обработки информации, к которым поставщик имеет доступ, использует или

управляет. Организация должна сохранять осведомленность о действиях, связанных с безопасностью, такими, как управление изменениями, выявление уязвимостей, а также оповещение об инцидентах информационной безопасности и ответных мерах в рамках установленного процесса информирования.

15.2.2 Управление изменениями в услугах поставщика

Метод реализации

Необходимо управлять изменениями в предоставлении услуг поставщиками, включая поддержание и улучшение существующих политик информационной безопасности, процедур и средств управления, с учетом критичности бизнес-информации, используемых систем и процессов и повторной оценки рисков.

Рекомендации по применению

Должны быть приняты во внимание следующие аспекты:

a) изменения в соглашениях с поставщиками;

b) изменения, производимые организацией для осуществления:
   1) улучшения предлагаемых в данный момент услуг;
   2) разработки любых новых приложений и систем;
   3) изменения или обновления политик и процедур организации;
   4) новых или измененных средств управления для разрешения инцидентов информационной безопасности и улучшения защиты;

c) изменения в услугах поставщика в целях:
   1) изменения и улучшения сетей;
   2) применения новых технологий;
   3) введения новых продуктов или новых версий/релизов;
   4) применения новых инструментов и сред разработки;
   5) изменения физического местонахождения обслуживающего оборудования;
   6) смены поставщиков;
   7) заключения контакта с другим субподрядчиком.

16 Управление инцидентами информационной безопасности

16.1 Управление инцидентами информационной безопасности и улучшения

Задача: гарантировать последовательный и результативный подход к управлению инцидентами информационной безопасности, включая информирование о событиях, связанных с безопасностью, и уязвимостях

16.1.1 Обязанности и процедуры

Метод реализации

Должны быть установлены обязанности руководства и процедуры, чтобы гарантировать быстрый, результативный и надлежащий ответ на инциденты информационной безопасности.

Рекомендации по применению

Должны быть приняты во внимание следующие рекомендации для установления обязанностей руководства и процедур, связанных с управлением инцидентами

информационной безопасности:

a) должны быть установлены обязанности руководства, чтобы гарантировать, что следующие процедуры разработаны и организация соответствующим образом о них оповещена:
   1) процедуры планирования и подготовки реакции на инцидент;
   2) процедуры мониторинга, обнаружения, анализа и информирования о событиях и инцидентах информационной безопасности;
   3) процедуры регистрации действий по управлению инцидентами;
   4) процедуры управления свидетельствами для суда;
   5) процедуры для оценки и принятия решения по событию информационной безопасности, а также оценке уязвимостей в информационной защите;
   6) процедуры ответных мер, включая передачу информации для принятия решения на более высоком уровне, управляемого восстановления после инцидента и информирования как персонала внутри организации, так и лиц за ее пределами;

b) установленная процедура должна гарантировать, что:
   1) проблемы, связанные с инцидентами информационной безопасности, решает компетентный персонал;
   2) контактный центр по вопросам обнаружения и информирования об инцидентах безопасности действует;
   3) соответствующие контакты с полномочными органами, внешними заинтересованными группами или форумами, которые посвящены вопросам, связанным с инцидентами информационной безопасности, поддерживаются;

c) процедуры отчетности должны включать в себя:
   1) разработку форм отчетности о событиях информационной безопасности для обеспечения действий по информированию и облегчения сотруднику выполнения всех необходимых мер, если произошло событие информационной безопасности;
   2) процедуру, которая должна быть выполнена, если произошло событие информационной безопасности, например, немедленное сообщение всех подробностей, таких, как вид несоответствия или нарушения, произошедший отказ, экранные сообщения и незамедлительное информирование контактного центра, а также принятие только скоординированных действий;
   3) ссылку на официально установленный процесс принятия дисциплинарных мер к сотрудникам, допустившим нарушения безопасности;
   4) работоспособные процессы обратной связи, гарантирующие, что лица, отвечающие за отчетность о событиях информационной безопасности, уведомлены о результатах после решения и закрытия проблемы.

Задачи по управлению инцидентами информационной безопасности должны быть согласованы с руководством и должно быть обеспечено понимание лицами, ответственными за управление инцидентами информационной безопасности, приоритетов организации в рамках обработки инцидентов информационной безопасности.

Дополнительная информация

Инциденты информационной безопасности могут быть и не локализованы в границах организации или государства. Для принятия мер в ответ на такие инциденты есть возрастающая необходимость в их координации и обмене информацией об этих инцидентах с другими организациями, в той мере, насколько это возможно.

Подробное руководство по управлению инцидентами информационной безопасности дано в ISO/IEC 27035 [20].

16.1.2 Оповещение о событиях, связанных с информационной безопасностью

Метод реализации

Оповещение о событиях информационной безопасности должно доводиться по соответствующим каналам управления как можно быстрее.

Рекомендации по применению

Все сотрудники и работающие по контракту должны быть ознакомлены со своей обязанностью сообщать о событиях информационной безопасности как можно быстрее. Они должны также знать процедуры передачи сообщения о событиях информационной безопасности и контакты, по которым сообщение о событии должно быть передано.

Ситуации, которые предполагают передачу сообщения о событии информационной безопасности, включают в себя:

a) нерезультативный контроль безопасности;
b) нарушение ожидаемого уровня целостности, конфиденциальности или возможности применения информации;
c) человеческие ошибки;
d) несоответствия политикам и инструкциям;
e) нарушение мер физической безопасности;
f) неконтролируемые изменение систем;
g) сбои в работе программного обеспечения или технических средств;
h) нарушение доступа.

Дополнительная информация

Сбои или иное несоответствующее поведение системы могут быть индикаторами атаки на систему защиты или нарушения защиты и, следовательно, о них всегда необходимо сообщать как о событиях информационной безопасности.

16.1.3 Оповещение об уязвимостях в информационной безопасности

Метод реализации

От сотрудников и работающих по контракту, использующих информационные системы и сервисы организации, необходимо требовать фиксировать и докладывать о любых обнаруженных или предполагаемых уязвимостях в информационной безопасности систем и сервисов.

Рекомендации по применению

Все сотрудники и работающие по контракту должны передавать сообщения, касающиеся уязвимостей в информационной безопасности, контактному центру как можно быстрее для того, чтобы предотвратить инциденты информационной безопасности. Механизм оповещения должен быть настолько простым, доступным и работоспособным, насколько это возможно.

Дополнительная информация

Сотрудникам и работающим по контракту должно быть рекомендовано не пытаться проверять предполагаемую уязвимость защиты. Тестирование уязвимости может быть воспринято как возможное ненадлежащие применение системы и может вызвать также повреждение в информационной системе или сервисе и привести к юридической ответственности лица, осуществлявшего тестирование.

16.1.4 Оценка и решение по событиям информационной безопасности

Метод реализации

События информационной безопасности должны оцениваться и затем приниматься решение, следует ли их классифицировать как инцидент информационной безопасности.

Рекомендации по применению

Контактный центр должен оценивать каждое событие информационной безопасности, используя согласованную классификационную шкалу событий и инцидентов информационной безопасности и принимать решение, должно ли событие быть классифицировано как инцидент информационной безопасности. Классификация и распределение инцидентов по приоритетам может помочь в определении влияния и масштаба инцидента.

В том случае, если в организации есть группа реагирования на инциденты информационной безопасности (ISIRT), оценка и принятие решения могут быть переданы ей для подтверждения или повторной оценки.

Результаты оценки и решений должны быть подробно зафиксированы с целью обращения к ним в будущем и проверки.

16.1.5 Ответные меры на инциденты информационной безопасности

Метод реализации

Реагирование на инциденты информационной безопасности должно осуществляться в соответствии с документированными процедурами.

Рекомендации по применению

Ответные меры на инциденты информационной безопасности должны приниматься назначенным контактным центром и другими соответствующими лицами в самой организации или в других организациях (см. 16.1.1).

Ответные меры должны включать следующее:

a) как можно более быстрый сбор свидетельств происшедшего;

b) проведение ретроспективного анализа, если требуется (см. 16.1.7);

c) передача решения на более высокий уровень, если требуется;

d) обеспечение того, что все выполняемые ответные действия соответствующим образом зарегистрированы для дальнейшего анализа;

e) оповещение об имеющем место инциденте информационной безопасности или его любых существенных деталях другим лицам, которые должны об этом знать в силу служебной необходимости, как в самой организации, так и в других организациях;

f) устранение уязвимости(ей) информационной безопасности, вызвавшей или способствовавшей возникновению инцидента;

g) официальное закрытие и документирование инцидента, после того, как он был успешно отработан.

Должен проводиться анализ после инцидента, если необходимо, для выявления причин инцидента.

Дополнительная информация

Первоочередной целью ответных мер на инцидент является возвращение «нормального уровня безопасности» и затем инициирование необходимого восстановления.

16.1.6 Излечение уроков из инцидентов информационной безопасности

Метод реализации

Знания, полученные из анализа и разрешения инцидентов информационной безопасности, должны использоваться для уменьшения вероятности инцидентов в будущем или их воздействия.

Рекомендации по применению

Должны быть внедрены механизмы для обеспечения возможности количественно определять и отслеживать виды, интенсивность и ущерб от инцидентов информационной безопасности. Информация, получаемая при оценке инцидентов информационной безопасности должна использоваться для выявления повторяющихся или существенно влияющих инцидентов.

Дополнительная информация

Оценка инцидентов информационной безопасности может указывать на необходимость улучшенных или дополнительных средств управления для снижения частоты, размера повреждений и ущерба в будущем или принята во внимание при пересмотре политики безопасности (см. 5.1.2).

С учетом вопросов конфиденциальности различные реальные истории, связанные с инцидентами информационной безопасности, могут быть использованы при обучении персонала (см. 7.2.2) как примеры, что может случиться, как реагировать на такие инциденты и как избежать их в будущем.

16.1.7 Сбор свидетельств

Метод реализации

Организация должна определить и применять процедуры для идентификации, сбора, комплектования и сохранения информации, которая может служить в качестве свидетельств.

Рекомендации по применению

Должны быть разработаны и затем выполняться внутренние процедуры обработки свидетельств с целью принятия мер дисциплинарного и юридического характера.

В общем случае эти процедуры должны обеспечивать процессы идентификации, сбора, комплектования и сохранения свидетельств в зависимости от типа носителей, устройств и состояния устройств, например, включенных или выключенных. Процедуры должны принимать во внимание:

a) порядок передачи и хранения;

b) сохранность свидетельств;

c) безопасность персонала;

d) роли и обязанности задействованного персонала;

e) компетентность персонала;

f) документацию;

g) инструктаж.

Там, где это возможно, должна быть предусмотрена сертификация или другие соответствующие средства оценки годности персонала и инструментария, для того, чтобы повысить ценность сохраненных свидетельств.

Свидетельства для судебного разбирательства могут быть за пределами организации или

границ юрисдикции. В этих случаях должно быть обеспечено наделение организации правом для сбора требуемой в качестве судебного свидетельства информации. Должны быть учтены требования различных юрисдикций, чтобы максимально увеличить шансы на признание в соответствующих юрисдикциях.

Дополнительная информация

Идентификация – это процесс, включающий поиск, признание и документирование возможного свидетельства. Сбор – это процесс собирания физических элементов, которые могут содержать потенциальное свидетельство. Комплектование – это процесс создания копий данных в рамках определенного набора. Сохранение – это процесс поддержания и защиты целостности и первоначального состояния потенциального свидетельства.

Когда инцидент информационной безопасности обнаружен впервые, неясно, приведет ли это событие к судебному разбирательству. Таким образом, существует опасность, что необходимое свидетельство будет намеренно или случайно уничтожено до того, как выяснится серьезность инцидента. Рекомендуется привлекать юриста или сотрудника полиции на ранней стадии при любых намеченных действиях юридического характера и прислушиваться к советам по поводу требуемых свидетельств.

Стандарт ISO/IEC 27037 [24] содержит указания по идентификации, сбору, комплектованию и сохранению цифровых свидетельств.

17 Аспекты информационной безопасности в менеджменте непрерывности бизнеса

17.1 Непрерывность информационной безопасности

Задача: Непрерывность информационной безопасности должна быть встроена в систему менеджмента непрерывностью бизнеса организации.

17.1.1 Планирование непрерывности информационной безопасности

Метод реализации

Организация должна определить свои требования к информационной безопасности и управлению непрерывностью информационной безопасности в неблагоприятных ситуациях, например, во время кризиса или чрезвычайной ситуации.

Рекомендации по применению

Организация должна определить, обеспечивается ли непрерывность информационной безопасности в рамках процесса менеджмента непрерывностью бизнеса или же в рамках процесса управления восстановлением после чрезвычайной ситуации. Требования информационной безопасности должны быть определены при планировании непрерывности бизнеса и восстановления после чрезвычайной ситуации.

В отсутствие официально утвержденных планов обеспечения непрерывности бизнеса и восстановления после чрезвычайной ситуации управление информационной безопасностью предполагает, что требования информационной безопасностью в неблагоприятных ситуациях остаются теми же самыми, что и в обычных условиях эксплуатации. Кроме того, организация может осуществлять анализ влияния аспектов информационной безопасности на бизнес, чтобы определить требования информационной безопасности, применимые в неблагоприятных ситуациях.

Дополнительная информация

Для снижения затрат времени и усилий на «дополнительный» анализ влияния

информационной безопасности на бизнес рекомендуется определять аспекты информационной безопасности в рамках общего менеджмента непрерывностью бизнеса или анализа влияния на бизнес в рамках управления восстановлением после чрезвычайной ситуации. Это предполагает, что требования непрерывности информационной безопасности четко сформулированы в рамках процессов управления непрерывностью бизнеса или управления восстановлением после чрезвычайной ситуации.

Информация по менеджменту непрерывностью бизнеса может быть найдена в стандартах ISO/IEC 27031 [14], ISO 22313 [9] и ISO 22301 [8].

17.1.2 Обеспечение непрерывности информационной безопасности

Метод реализации

Организация должна установить, документировать, внедрить и поддерживать процессы, процедуры и средства управления, чтобы гарантировать необходимый уровень непрерывности информационной безопасности во время неблагоприятной ситуации.

Рекомендации по применению

Организация должна гарантировать, что

a) внедрена соответствующая структура управления для подготовки к, минимизации и ответных мер на дезорганизующее событие с участием персонала, обладающего необходимыми полномочиями, опытом и компетентностью;

b) назначен для ответных мер по инциденту персонал с необходимой ответственностью, полномочиями и компетентностью для управления инцидентом и обеспечения информационной безопасности;

c) разработаны и утверждены документированные планы, процедуры ответных мер и восстановления, детализирующих, каким образом организация будет справляться с дезорганизующим событием и обеспечивать свою информационную безопасность на запланированном уровне, ориентируясь на одобренные руководством цели по обеспечению непрерывности информационной безопасности (см. 17.1.1).

В соответствии с требованиями обеспечения непрерывности информационной безопасности организация должна установить, документировать, внедрить и обеспечивать работоспособность:

a) средств управления информационной безопасностью в рамках процессов обеспечения непрерывности бизнеса или восстановления после чрезвычайных ситуаций, процедур и обеспечивающих систем и инструментов;

b) процессов, процедур и осуществления изменений для поддержки существующих средств управления информационной безопасностью пока длится негативная ситуация;

c) компенсирующие меры для тех средств управления информационной безопасностью, работоспособность которых не может быть обеспечена при неблагоприятной ситуации.

Дополнительная информация

В рамках контекста обеспечения непрерывности бизнеса или восстановления после чрезвычайной ситуации могли быть определены конкретные процессы и процедуры. Информация, которая обрабатывается при выполнении этих процессов и процедур или в специализированных информационных системах для их поддержки, должна быть защищена. Следовательно, организация должна привлекать специалистов по информационной безопасности при разработке, внедрении и функционировании процессов и процедур обеспечения непрерывности бизнеса и восстановления после чрезвычайной ситуации.

Внедренные средства управления информационной безопасностью должны продолжать

функционировать при возникновении неблагоприятной ситуации. Если средства управления безопасностью не способны продолжать обеспечивать безопасность информации, должны быть разработаны, внедрены и поддерживаться в рабочем состоянии другие средства управления для обеспечения приемлемого уровня информационной безопасности.

17.1.3 Проверка, анализ и оценка непрерывности информационной безопасности

Метод реализации

Организация должна проверять разработанные и внедренные средства управления непрерывностью информационной безопасности через определенные интервалы времени, чтобы гарантировать, что эти средства пригодны и результативны во время неблагоприятных ситуаций.

Рекомендации по применению

Организационные, технические, процедурные изменения или изменения в процессах в контексте ли эксплуатации, или обеспечения непрерывности могут вести к изменениям требований непрерывности информационной безопасности. В таких случаях целостность процессов, процедур и средств управления информационной безопасностью должна быть проанализирована с точки зрения этих измененных требований.

Организации должны проверять непрерывность управления информационной безопасностью посредством:

a) опробования и тестирования функциональности процессов, процедур и средств управления непрерывностью информационной безопасности, чтобы гарантировать, что они соответствуют целям обеспечения непрерывности информационной безопасности;
b) опробования и тестирования данных и порядка выполнения процессов, процедур и средств управления непрерывностью информационной безопасности, чтобы гарантировать, что результаты их осуществления соответствует целям обеспечения непрерывности информационной безопасности;
c) анализа пригодности и результативности мер обеспечения непрерывности информационной безопасности при изменении информационных систем, процессов обеспечения информационной безопасности, процедур и средств управления или процессов управления непрерывностью бизнеса/восстановлением после чрезвычайных ситуаций, а также применяемых решений.

Дополнительная информация

Проверка средств управления непрерывностью информационной безопасности отличается от общей проверки информационной безопасности и должна выполняться вне рамок тестирования изменений. Если возможно, предпочтительнее объединить проверку средств управления непрерывностью информационной безопасностью с тестами обеспечения организацией непрерывности бизнеса или восстановления после чрезвычайных ситуаций.

17.2 Резервирование

Задача: гарантировать возможность применения средств обработки информации.

17.2.1 Возможность применения средств обработки информации

Метод реализации

Средства обработки информации должны устанавливаться с избыточностью, достаточной для обеспечения требований по возможности применения.

Рекомендации по применению

Организация должна определить бизнес-требования к возможности применения информационных систем. Там, где возможность применения не может быть гарантирована использованием существующей системной архитектуры, должен быть рассмотрен вариант резервирования.

Где это применимо, резервные информационные системы должны быть проверены, чтобы гарантировать, что переход с одного компонента на другой работает, как запланировано.

Дополнительная информация

Введение избыточности может приводить к рискам для целостности или конфиденциальности информации и информационных систем, которые необходимо учитывать при проектировании информационных систем.

18 Соответствие

18.1 Соответствие законодательным и контрактным требованиям

Задача: избегать нарушений законодательных, нормативных или контрактных обязательств, имеющих отношение к информационной безопасности, и любых требований безопасности.

18.1.1 Определение действующих законодательных и контрактных требований

Метод реализации

Все соответствующие законодательные, нормативные, контрактные требования, а также подход организации к удовлетворению этих требований должны быть явным образом определены, документированы и сохраняться актуальными для каждой информационной системы и организации.

Рекомендации по применению

Конкретные средства управления и персональные обязательства выполнять эти требования должны также быть определены и документированы.

Руководители должны определить все законодательные акты, действующие в их организации, для того, чтобы выполнять требования, предъявляемые для данного вида бизнеса. Если организация ведет бизнес в других странах, руководители должны иметь в виду выполнение требований во всех соответствующих странах.

18.1.2 Права интеллектуальной собственности

Метод реализации

Должны выполняться соответствующие процедуры, чтобы гарантировать соответствие законодательным, нормативным и контрактным требованиям, связанным с правами на интеллектуальную собственность и использованием программных продуктов, защищенных авторским правом.

Рекомендации по применению

Для защиты любого материала, который может рассматриваться как интеллектуальная собственность, необходимо принять во внимание следующие рекомендации:

a) обнародование политики в области соблюдения прав интеллектуальной собственности, которая определяет законное применение программного обеспечения и информационных продуктов;

b) получение программного обеспечения только из известных и надежных источников,

чтобы гарантировать, что авторские права не нарушены;

c) обеспечение осведомленности о политиках по защите прав интеллектуальной собственности и предупреждение о решимости предпринимать меры дисциплинарного воздействия к тем, кто нарушает их;

d) поддержание в актуальном состоянии соответствующих реестров активов и выявление всех активов, в отношении которых действует требование по защите прав интеллектуальной собственности;

e) сохранение доказательства и свидетельства обладания лицензиями, мастер-дисками, руководствами и т.д.;

f) выполнение средств управления, чтобы гарантировать, что любое максимально разрешенное лицензией количество пользователей не превышено;

g) проведение проверок на предмет того, что установлены только авторизованное программное обеспечение и лицензионные продукты;

h) разработка политики для обеспечения выполнения условий лицензий;

i) разработка политики для утилизации или передачи программного обеспечения другим;

j) соответствие условиям и ограничениям для программного обеспечения и информации, полученных из сетей общего пользования;

k) не копировать, не конвертировать в другой формат и не извлекать из коммерческих медиа-продуктов (фильм, аудиозапись) ничего, кроме того, что разрешено законом об авторских правах;

l) не копировать полностью или частично книги, статьи, отчетные материалы или иные документы, кроме того, что разрешено законом об авторских правах.

Дополнительная информация

Права на интеллектуальную собственность включают в себя авторские права на программное обеспечение или документы, права разработчика, торговые марки, патенты и лицензии на исходный код.

Программные продукты, защищенные авторским правом, поставляются обычно с лицензионным соглашением, которое определяет положения и условия лицензии, например, ограничение использования продуктов только конкретными устройствами или ограничение копирования только созданием резервных копий. Важность и осознание прав интеллектуальной собственности на программное обеспечение, разрабатываемое в организации, должны быть доведены до персонала.

Законодательные, нормативные и контрактные требования могут устанавливать ограничения на копирование материалов, защищенных авторским правом. В частности, они могут требовать, чтобы использовались только материалы, разработанные организацией, или лицензированные, или полученные организацией от разработчика. Нарушение авторского права может вести к юридическим последствиям, которые могут предусматривать штрафы и уголовное преследование.

18.1.3 Защита записей

Метод реализации

Записи должны быть защищены от потери, повреждения, фальсификации, несанкционированного доступа и несанкционированной публикации в соответствии с законодательными, нормативными, контрактными требованиями и требованиями бизнеса.

Рекомендации по применению

При решении вопросов, связанных с защитой конкретных записей организации, необходимо рассмотреть их соответствующую классификацию, основанную на схеме классификации организации. Записи должны быть распределены по категориям разных типов, например, учетные записи, записи базы данных, журналы транзакций, контрольные журналы и операционные процедуры, каждый со своим сроком хранения и типом допустимого носителя для хранения, например, бумага, микрофиши, магнитные и оптические носители. Любые связанные криптографические ключи и программы, связанные с зашифрованными архивами, или цифровые подписи (см. раздел 10) должны также сохраняться в течение срока хранения с возможностью дешифрации записей.

Должна быть учтена возможность ухудшения качества носителя, используемого для хранения записей.

Процедуры хранения и обработки должны выполняться в соответствии с рекомендациями производителя.

В тех случаях, когда выбран электронный носитель, должны быть разработаны процедуры, чтобы гарантировать возможность доступа к данным (как в физическом смысле, так и в части читаемости формата) в течение всего срока хранения с защитой от потери при технологических изменениях в будущем.

Системы хранения данных должны быть выбраны так, чтобы требуемые данные могли быть получены в приемлемое время и приемлемом формате, в зависимости от требований, которые должны быть выполнены.

Система хранения и обработки должна гарантировать идентификацию записей и их сроков хранения, как это определено национальным или региональным законодательством или нормами, если это применимо. Эта система должна допускать соответствующую ликвидацию записей по истечении срока хранения, если они более не востребованы организацией.

Чтобы выполнить эти задачи по защите записей, в организации должны быть предприняты следующие шаги:

a) должны быть выпущены руководства по срокам хранения, хранению, обработке и ликвидации записей и информации;

b) должен быть разработан порядок хранения с указанием записей и их сроков хранения;

c) должен храниться реестр источников ключевой информации.

Дополнительная информация

Некоторые записи могут требовать защищенного хранения для выполнения законодательных, нормативных или контрактных требований, а также для обеспечения существенно важной бизнес-деятельности. Примером являются записи, которые могут требоваться, как свидетельства того, что организация работает в пределах, установленных законом, или нормативных правил, чтобы обеспечить защиту от возможного преследования в рамках гражданского или уголовного права, или чтобы подтвердить финансовый статус организации ее заинтересованным лицам, внешним сторонам и аудиторам. Национальное законодательство или нормы могут устанавливать период хранения и содержание для хранимой информации.

Дополнительная информация об управлении записями организации может быть найдена в ISO 15489-1 [5].

18.1.4 Конфиденциальность и защита персональных данных

Метод реализации

Конфиденциальность и защита персональных данных должны быть обеспечены в той мере, в какой это требуется соответствующим законодательством и нормативными актами, где это применимо.

Рекомендации по применению

Должна быть разработана и внедрена политика организации в отношении конфиденциальности и защиты персональных данных. Эта политика должна быть доведена до всех, кто участвует в обработке персональных данных.

Следование этой политике и всем соответствующим законодательным актам и нормам, связанным с защитой частной жизни людей и персональных данных, требует соответствующей управленческой структуры и контроля. Часто это наилучшим образом достигается назначением ответственного лица, например, ответственного за охрану личной информации, который должен разработать инструкцию для руководителей, пользователей и поставщиков услуг, определяющую их персональные обязанности и конкретные процедуры, которым необходимо следовать. Назначение ответственности за обработку персональных данных и обеспечение знания принципов сохранения конфиденциальности должны быть осуществлены в соответствии с действующим законодательством и нормами. Должны быть выполнены соответствующие технические и организационные мероприятия по защите персональной информации.

Дополнительная информация

Стандарт ISO 29100 [25] представляет высокоуровневую концепцию защиты персональной информации в применении к системам информационно-коммуникационных технологий. Немало стран уже ввели законодательные акты, устанавливающие механизмы сбора, обработки и передачи персональных данных (обычно это информация о здравствующих людях, которые могут быть идентифицированы на основании этой информации). В зависимости от соответствующего национального законодательства такие механизмы могут налагать обязанности на тех, кто собирает, обрабатывает и рассылает персональную информацию, а также могут ограничивать возможность передачи персональной информации в другие страны.

18.1.5 Регламентация применения криптографических средств

Метод реализации

Криптографические методы должны использоваться в соответствии со всеми действующими соглашениями, законодательными и нормативными актами.

Рекомендации по применению

Для соответствия действующим соглашениям, законодательным и нормативным актам необходимо учесть следующее:

a) ограничения на импорт и экспорт компьютерной техники и программного обеспечения, осуществляющего криптографические функции;

b) ограничения на импорт и экспорт компьютерной техники и программного обеспечения, которые разработаны с возможностью добавления в них криптографических функций;

c) ограничения на применение шифрования;

d) принудительно или добровольно применяемые методы доступа органов государственной власти к информации, зашифрованной устройствами или программным обеспечением для защиты конфиденциальности содержания.

Необходимо заручиться юридической поддержкой, чтобы гарантировать соответствие действующим соглашениям, законодательным и нормативным актам. До того, как зашифрованная информация или криптографические средства будут перемещены из одной юрисдикции в другую, должны быть получены юридические рекомендации.

18.2 Анализ информационной безопасности

Задача: гарантировать, что средства обеспечения информационной безопасности внедрены и используются в соответствии с организационной политикой и процедурами.

18.2.1 Независимый анализ информационной безопасности

Метод реализации

Подход организации к управлению информационной безопасностью и его реализация (т. е. задачи управления, средства управления, политики, процессы и процедуры по обеспечению информационной безопасности) должны подвергаться независимому анализу через запланированные интервалы времени или в тех случаях, когда происходят существенные изменения.

Рекомендации по применению

Руководство должно инициировать проведение независимого анализа. Такого рода независимый анализ необходим, чтобы гарантировать постоянную пригодность, адекватность и результативность подхода организации к управлению информационной безопасностью. Анализ должен включать в себя оценку возможностей для улучшения и необходимости изменений в подходе к безопасности, в том числе политике и задачах управления.

Такой анализ должен проводиться людьми, не связанными с анализируемой областью, например, теми, кто проводит внутренние аудиты, руководителями других направлений или внешней организацией, специализирующейся на подобного рода оценках. Те, кто проводит такие проверки, должен обладать соответствующими навыками и опытом.

Результаты независимого анализа должны быть зафиксированы и переданы руководству, инициировавшему анализ. Эти записи должны сохраняться.

Если независимый анализ выявляет неадекватность подхода к управлению информационной безопасностью и его реализации в организации, например, документированные задачи и требования не выполняются или не согласуются с положениями, сформулированными в политиках информационной безопасности (см. 5.1.1), руководство должно рассмотреть необходимость корректирующих действий.

Дополнительная информация

Стандарты ISO/IEC 27007 [12] «Руководство по аудиту системы менеджмента информационной безопасности» и ISO/IEC TR 27008 [13] «Руководство для аудиторов по проверке средств управления информационной безопасностью» также дают рекомендации по проведению независимого анализа.

18.2.2 Соответствие политикам безопасности и стандартам

Метод реализации

Руководители в пределах своей области ответственности должны регулярно анализировать соответствие обработки информации и процедур политикам безопасности, стандартам и любым другим требованиям по безопасности.

Рекомендации по применению

Руководители должны определить, каким образом анализировать выполнение требований

информационной безопасности, определенных в политиках, стандартах и других действующих нормах. Необходимо рассмотреть возможность применение инструментов автоматизированного измерения и формирования отчетов для обеспечения эффективного регулярного анализа.

В случае выявления в результате анализа любого несоответствия, руководители должны:

a) определить причины несоответствия;

b) оценить необходимость действий для обеспечения соответствия;

c) выполнить соответствующие корректирующие действия;

d) оценить результативность предпринятых корректирующих действий и выявить любые недостатки и слабости.

Результаты анализа и корректирующих действий, осуществленных руководителями, должны быть зафиксированы и эти записи должны сохраняться. Руководители должны передавать эти результаты лицам, которые выполняют независимый анализ (см. 18.2.1), когда такой анализ проводится в сфере их ответственности.

Дополнительная информация

Применение систем оперативного мониторинга описано в 12.4.

18.2.3 Анализ технического соответствия

Метод реализации

Информационные системы должны регулярно анализироваться на соответствие политикам и стандартам информационной безопасности организации.

Рекомендации по применению

Техническое соответствие должно анализироваться преимущественно с помощью автоматизированных инструментов, которые генерируют отчеты для последующей их интерпретации техническим специалистом. Кроме этого, анализ может выполняться вручную (с использованием соответствующих программных средств, если необходимо) опытным системным инженером.

Если применяются тесты на проникновение или оценки уязвимостей, то необходимо делать предупреждение, так как такая активность может вести к нарушению безопасности системы. Такие тесты должны планироваться, документироваться и повторяться.

Любой анализ технического соответствия должен выполняться только компетентными и авторизованными лицами или под управлением таких лиц.

Дополнительная информация

Анализ технического соответствия включает проверку действующих систем, чтобы гарантировать, что средства управления оборудованием и программным обеспечением осуществляются надлежащим образом. Данный тип анализа соответствия требует специалиста по технической экспертизе.

Анализ соответствия также включает в себя, например, тест на проникновение и оценку уязвимостей, которые могут выполняться независимыми экспертами, приглашенными для этих целей. Это может быть полезным при определении уязвимостей в системе и для проверки, насколько результативны средства управления в предупреждении неавторизованного доступа с использованием этих уязвимостей.

Тест на проникновение и оценка уязвимостей дает мгновенный снимок системы в конкретном состоянии на конкретный момент времени. Это представление ограничено той частью системы, которая подвергалась тестированию при попытках проникновения. Тест на

проникновение и оценка уязвимостей не заменяют собой оценки рисков.

Стандарт ISO/IEC 27008 [13] дает конкретные рекомендации, связанные с анализом технического соответствия.

Библиография

[1] ISO/IEC 27002:2013, Information technology — Security Techniques — Code of practice for information security controls

[2] ISO/IEC 27003, Information technology — Security techniques — Information security management system implementation guidance

[3] ISO/IEC 27004, Information technology — Security techniques — Information security management — Measurement

[4] ISO/IEC 27005, Information technology — Security techniques — Information security risk management

[5] ISO 31000:2009, Risk management — Principles and guidelines

[6] ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, 2012