ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27011–2012

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002

ISO/IEC 27011:2008

Information technology – Security techniques –

Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

(IDT)

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184–ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации – ГОСТ Р 1.0–2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Федерального агентства по техническому регулированию и метрологии от 24 сентября 2012 г. № 424-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27011:2008 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002» (ISO/IEC 27011:2008, Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002)

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5–2004 (пункт 3.5)

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок – в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомления и тексты размещаются также в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию метрологии в сети Интернет

© Стандартинформ, 2013

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

Содержание

1 Область применения
2 Нормативные ссылки
3 Термины, определения и сокращения
3.1 Термины и определения
3.2 Сокращения
4 Обзор
4.1 Структура данного руководства
4.2 Системы менеджмента информационной безопасности в телекоммуникационном бизнесе
5 Политика безопасности
6 Организационные аспекты информационной безопасности
6.1 Задачи, решаемые внутри организации
6.2 Аспекты взаимодействия со сторонними организациями
7 Менеджмент активов
7.1 Ответственность за активы
7.2 Классификация информации
8 Безопасность, связанная с персоналом
8.1 Перед трудоустройством
8.2 В течение занятости
8.3 Прекращение или смена занятости
9 Физическая безопасность и защита от воздействий окружающей среды
9.1 Зоны безопасности
9.2 Безопасность оборудования
10 Менеджмент коммуникаций и работ
10.1 Эксплуатационные процедуры и обязанности
10.2 Менеджмент оказания услуг третьей стороной
10.3 Планирование и приемка систем
10.4 Защита от вредоносной и мобильной программы

10.5 Резервирование
10.6 Менеджмент безопасности сети
10.7 Обращение с носителями информации
10.8 Обмен информацией
10.9 Услуги электронной торговли
10.10 Мониторинг
11 Управление доступом
11.1 Требования бизнеса по управлению доступом
11.2 Менеджмент доступа пользователей
11.3 Обязанности пользователя
11.4 Управление доступом к сети
11.5 Управление доступом к эксплуатируемой системе
11.6 Управление доступом к информации и прикладным программам
11.7 Мобильная вычислительная техника и дистанционная работа
12 Приобретение, разработка и эксплуатация информационных систем
12.1 Требования безопасности информационных систем
12.2 Корректная обработка в прикладных программах
12.3 Криптографические меры и средства контроля и управления
12.4 Безопасность системных файлов
12.5 Безопасность в процессах разработки и поддержки
12.6 Менеджмент технических уязвимостей
13 Менеджмент инцидентов информационной безопасности
13.1 Оповещение о событиях и уязвимостях информационной безопасности
13.2 Менеджмент инцидентов информационной безопасности и необходимое совершенствование
14 Менеджмент непрерывности бизнеса
14.1 Аспекты информационной безопасностью в рамках менеджмента непрерывности бизнеса

15 Соответствие .....

Приложение А (обязательное) Дополнительный перечень мер и средств контроля и управления для телекоммуникаций .....

Приложение В (справочное) Дополнительные рекомендации по реализации .....

Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации .....

Библиография .....

Введение

Настоящий национальный стандарт предоставляет дополнительные рекомендации по реализации и менеджменту информационной безопасности в телекоммуникационных организациях на основе ИСО/МЭК 27002 (Свод норм и правил менеджмента информационной безопасности). Помимо целей безопасности, мер и средств контроля и управления, описанных в ИСО/МЭК 27002, телекоммуникационные организации должны принимать во внимание следующие аспекты безопасности:

1) *конфиденциальность*. Информация, имеющая отношение к телекоммуникационным организациям, должна быть защищена от несанкционированного раскрытия.

Это означает неразглашение сведений о наличии, содержании, источнике, адреса назначения, а также даты и времени переданной информации.

Для телекоммуникационных организаций крайне важно обеспечить уверенность в том, что неразглашение информации о коммуникациях не нарушалось. Лица, нанимаемые на работу телекоммуникационными организациями, должны поддерживать конфиденциальность любой информации о других лицах, которая могла стать им известна в ходе выполнения их служебных обязанностей.

Примечание — В некоторых странах термин «тайна сообщений» используется в контексте «неразглашения информации о соединениях»;

2) *целостность*. Установка и использование телекоммуникационных средств должны находиться под контролем, обеспечивающим уверенность в подлинности, точности и полноте информации, переданной, отправленной или полученной с помощью проводной связи, радиосвязи или любыми другими способами;

3) *доступность*. При необходимости должен обеспечиваться только санкционированный доступ к телекоммуникационной информации, оборудованию и среде, которые используются для предоставления услуг связи, обеспечиваемых с помощью проводной связи, радиосвязи или любыми другими способами. В качестве расширения доступности телекоммуникационные организации должны отдавать приоритет важнейшим коммуникациям в случае чрезвычайной ситуации, а также соблюдать нормативные требования.

Менеджмент информационной безопасности в телекоммуникационных организациях необходим независимо от используемого метода, например, применения

проводных, беспроводных или широкополосных технологий. Если менеджмент информационной безопасности не реализован надлежащим образом, уровень риска телекоммуникаций в отношении конфиденциальности, целостности и доступности может возрасти.

Телекоммуникационные организации предназначены для предоставления телекоммуникационных услуг, с выполнением роли посредника по передаче информации с помощью оборудования, используемого для установления соединений. Поэтому следует учитывать, что доступ и использование средств обработки информации в телекоммуникационной организации осуществляется не только ее собственными служащими и подрядчиками, но также различными пользователями вне организации.

Для предоставления телекоммуникационных услуг, телекоммуникационным организациям для обеспечения взаимодействия необходимо обеспечить либо коллективное использовании своих телекоммуникационных услуг и оборудования, либо использовать телекоммуникационные услуги и оборудование других телекоммуникационных организаций. Соответственно, менеджмент информационной безопасности в телекоммуникационных организациях является взаимозависимым и может включать любую или все сферы сетевой инфраструктуры, услуг, прикладных программ и других средств.

Независимо от масштаба операций, зоны обслуживания или видов услуг телекоммуникационные организации должны реализовывать соответствующие меры и средства контроля и управления для обеспечения конфиденциальности, целостности, доступности и любых других свойств безопасности телекоммуникаций.

Аудитория

Данный национальный стандарт предоставляет телекоммуникационным организациям и лицам, отвечающим за информационную безопасность, наряду с поставщиками средств защиты, аудиторами, поставщиками телекоммуникационных терминалов и используемыми контент-провайдерами, наряду с общим набором основных целей управления безопасностью на основе ИСО/МЭК 27002 и также характерные для телекоммуникационного сектора меры и средства контроля и управления, , рекомендации по менеджменту информационной безопасности, предусматривающие выбор и реализацию таких мер и средств контроля и управления.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002

Information technology. Security techniques. Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

Дата введения – 2014-01-01

1 Область применения

Настоящий национальный стандарт определяет рекомендации, поддерживающие реализацию менеджмента информационной безопасности в телекоммуникационных организациях.

Применение данного национального стандарта позволит телекоммуникационным организациям выполнять базовые требования менеджмента информационной безопасности в отношении конфиденциальности, целостности, доступности и любых других аспектов безопасности.

2 Нормативные ссылки

Настоящий национальный стандарт содержит положения, основанные на рекомендациях действующих стандартов. Однако все рекомендации и стандарты подлежат пересмотру, поэтому перед использованием данного национального стандарта следует изучить последнюю редакцию перечисленных ниже стандартов. Члены МЭК и ИСО поддерживают каталоги действующих международных стандартов. Бюро стандартизации электросвязи МСЭ (международного союза электросвязи) поддерживает каталог действующих в настоящее время рекомендаций МСЭ-Т.

Издание официальное

ИСО/МЭК 27001:2005 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements)

ИСО/МЭК 27002:2005 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности (ISO/IEC 27002:2005, Information technology – Security techniques – Code of practice for information security management)

3 Термины, определения и сокращения

3.1 Термины и определения

Для целей данного национального стандарта применяются термины и определения, приведенные в ИСО/МЭК 27002. Кроме того, применяются следующие термины и определения:

3.1.1 **совместное размещение** (collocation): Установка телекоммуникационных средств в помещениях других поставщиков телекоммуникационных услуг.

3.1.2 **узел связи** (communication centre): Сооружение, где размещаются средства для обеспечения телекоммуникационного бизнеса.

3.1.3 **важнейшие коммуникации** (essential communications): Коммуникации, которые требуются для предупреждения бедствий или оказания помощи, для поддержки транспорта, связи, энергоснабжения или для поддержания общественного порядка.

3.1.4 **неразглашение [информации о] соединениях** (non-disclosure of communications): Особенности соединений, обслуживаемых лицами, нанятыми на работу телекоммуникационной организацией, не должны разглашаться с точки зрения наличия, содержания, источника, адреса назначения, даты и времени переданной информации.

3.1.5 **персональная информация** (personal information): Информация о лице, которая может быть использована для идентификации этого лица. Конкретная информация, используемая для такой идентификации, определяется национальным законодательством.

3.1.6 **приоритетный вызов** (priority call): Телекоммуникации, осуществляемые специальными терминалами при чрезвычайных ситуациях, которые требуют приоритетной обработки, ограничивая общественные вызовы. Специальные терминалы могут предоставлять различные услуги (передача голоса по IP-сетям, передача голоса по ТфОП, IP-трафик данных и т. д.) для проводных и беспроводных сетей.

3.1.7 **телекоммуникационные прикладные программы** (telecommunications applications): Прикладные программы, например, электронная почта, к которым получают доступ конечные пользователи и которые базируются на сетевых услугах.

3.1.8 **телекоммуникационный бизнес** (telecommunications business): Бизнес по предоставлению телекоммуникационных услуг с целью удовлетворения потребностей других лиц.

3.1.9 **телекоммуникационная аппаратная** (telecommunications equipment room): Часть общей площади, где расположено оборудование для обеспечения телекоммуникационного бизнеса.

3.1.10 **телекоммуникационные средства** (telecommunications facilities): Устройства, оборудование, провода и кабели, физические сооружения или другое электрооборудование для функционирования телекоммуникаций.

3.1.11 **телекоммуникационные организации** (telecommunications organizations): Коммерческая организация, предоставляющая телекоммуникационные услуги с целью удовлетворения потребностей других лиц.

3.1.12 **телекоммуникационные записи** (telecommunications records): Информация, касающаяся участвующих в соединении сторон, исключая содержание, время и длительность состоявшейся телекоммуникации.

3.1.13 **телекоммуникационные услуги** (telecommunications services): Передача информации с использованием телекоммуникационных средств или иных средств обеспечения передачи между пользователями телекоммуникационных услуг или между клиентами телекоммуникационных услуг.

3.1.14 **клиент телекоммуникационных услуг** (telecommunications service customer): Лицо или организация, заключившая договор с телекоммуникационными организациями о предлагаемых ими телекоммуникационных услугах.

3.1.15 **пользователь телекоммуникационных услуг** (telecommunications service user): Лицо или организация, использующие телекоммуникационные услуги.

3.1.16 **терминальное оборудование** (terminal facilities): Телекоммуникационные средства, которые подключены к одному концу оборудования телекоммуникационной линии связи и часть которого устанавливается в том же помещении (включая площадки, рассматриваемые как помещения) или в том же здании, где установлены любые другие части оборудования телекоммуникационной линии связи.

3.1.17 **пользователь** (user): Лицо или организация, использующие средства или системы обработки информации, например, сотрудник, подрядчик или пользователь третьей стороны.

3.2 Сокращения

Для целей данного национального стандарта применяются следующие сокращения:

ADSL – асимметричная цифровая абонентская линия (asymmetric digital subscriber line);

ASP – поставщик услуг по аренде прикладных программ (application service provider);

CATV – кабельное телевидение (community antenna TeleVision);

CERT – группа реагирования на компьютерные инциденты (computer emergency response team);

DDoS – распределенный отказ в обслуживании (distributed denial of service);

DNS – служба имен доменов (domain name system);

DoS – отказ в обслуживании (denial of service);

ISAC – центр обмена и анализа информации (information sharing and analysis centre);

NGN – сети следующего поколения (next generation network);

NMS – система сетевого менеджмента (network management system);

OAM&P – эксплуатация, администрирование, обслуживание и предоставление (operations, administration, maintenance and provisioning);

SIP – протокол инициации сессии (session initiation protocol);

SLA – соглашение об уровне услуг (service level agreement);

SOA – положение о применимости (statement of applicability);

URL – унифицированный указатель ресурса (uniform resource locator);

VoIP – передача голоса по IP сетям (voice over internet protocol);

ИБП – источник бесперебойного питания (UPS – uninterruptible power supply);

ИТ – информационные технологии;

ПИН – персональный идентификационный номер (PIN – personal identification number);

СМИБ – система менеджмента информационной безопасности (ISMS – information security management system);

ТфОП – коммутируемая телефонная сеть общего пользования (PSTN - public switched telephone network).

4 Обзор

4.1 Структура данного руководства

Данный национальный стандарт имеет структуру, сходную с ИСО/МЭК 27002. В тех случаях, когда определенные в ИСО/МЭК 27002 цели и меры и средства контроля и управления применимы без какой-либо дополнительной информации, дается только ссылка на ИСО/МЭК 27002. Характерная для телекоммуникационного сектора совокупность мер и средств контроля и управления, а также рекомендаций описана в Приложении А (обязательном).

В тех случаях, когда меры и средства контроля и управления требуют дополнительной характерной для телекоммуникаций рекомендации по реализации, мера и средство контроля и управления, а также и рекомендация по их реализации повторяются из ИСО/МЭК 27002 без изменений, а за ними следует характерная для телекоммуникаций рекомендация, связанная с этой мерой и средством контроля и управления. Характерные для телекоммуникационного сектора рекомендации и информация включены в следующие разделы:

- Организационные аспекты информационной безопасности (раздел 6);
- Менеджмент активов (раздел 7);
- Безопасность, связанная с персоналом (раздел 8);
- Физическая безопасность и защита от воздействий окружающей среды (раздел 9);
- Менеджмент коммуникаций и работ (раздел 10);
- Управление доступом (раздел 11);
- Приобретение, разработка и эксплуатация информационных систем (раздел 12);
- Менеджмент инцидентов информационной безопасности (раздел 13);
- Менеджмент непрерывности бизнеса (раздел 14).

4.2 Системы менеджмента информационной безопасности в телекоммуникационном бизнесе

4.2.1 Цель

Информация, как и другие активы организации, является важным фактором для бизнеса организации. Информация может быть напечатана или записана на бумаге, сохранена в электронном виде, отправлена по почте, передана в электронном виде, показана в фильме или высказана в беседах. Независимо от формы или функциональности информации или средств, используемых для обмена информацией или ее хранения, информация всегда требует соответствующей защиты.

Организации и их информационные системы и сети сталкиваются с угрозами безопасности, исходящими из широкого спектра источников, включая мошенничество с использованием компьютера, шпионаж, вредительство, вандализм, утечку информации, землетрясение, пожар или затопление. Эти угрозы безопасности могут возникать внутри или вне телекоммуникационных организаций, причиняя ущерб организации.

При нарушении информационной безопасности, например, в результате несанкционированного доступа к системе обработки информации, организация может понести ущерб. Поэтому для организации необходимо обеспечивать информационную безопасность, постоянно совершенствуя свою систему

менеджмента информационной безопасности (СМИБ) в соответствии с ИСО/МЭК 27001.

Эффективная информационная безопасность достигается посредством реализации соответствующей совокупности мер и средств контроля и управления, основанной на тех, что описаны в данном национальном стандарте. Эти меры и средства контроля и управления необходимо устанавливать, реализовывать, подвергать мониторингу, проверять и совершенствовать в телекоммуникационных средствах, услугах и прикладных программах. Успешное развертывание мер и средств контроля и управления безопасностью создаст лучшую возможность достижения соответствия целям безопасности и для успешного бизнеса организации.

Телекоммуникационные организации, чьи средства используются различными пользователями для обработки такой информации, как персональные данные, конфиденциальные данные и бизнес-данные, должны обращаться с этой информацией с большой/должной заботой и применять соответствующий уровень защиты.

В заключение следует сказать, что телекоммуникационным организациям необходимо создать и непрерывно совершенствовать общую СМИБ, что обеспечит уверенность в поддержке соответствующих мер и средств контроля и управления безопасностью.

4.2.2 Вопросы безопасности в телекоммуникациях

Требования к общей структуре безопасности в телекоммуникациях проистекают из разных источников:

a) клиенты/абоненты, нуждающиеся в доверии к сетям и предоставляемым услугам, включая доступность услуг (особенно экстренных служб) в случае серьезных катастроф;

b) органы государственной власти, требующие обеспечения безопасности в соответствии с директивами, нормами и законами для обеспечения уверенности в доступности услуг, в честной конкуренции и в защите персональной информации;

c) сетевые операторы и поставщики услуг, нуждающиеся в обеспечении безопасности для защиты своих практических интересов и интересов бизнеса, а также для выполнения своих обязательств перед клиентами и обществом.

Кроме того, телекоммуникационные организации должны учитывать следующие инциденты, связанные с окружающей средой и безопасностью эксплуатации:

a) телекоммуникационные услуги в большой степени зависят от различных взаимосвязанных средств связи, таких как маршрутизаторы, коммутаторы, серверы доменных имен, ретрансляторы систем передачи и системы сетевого менеджмента (NMS). Соответственно, проблемы безопасности телекоммуникаций могут возникать в различном оборудовании/средствах и быстро распространяться через сеть на другое оборудование/средства;

b) в дополнение к телекоммуникационным средствам к серьезным нарушениям безопасности могут приводить также уязвимости сетевых протоколов и топологии сети. В частности конвергенция проводных и беспроводных сетей в сетях следующего поколения (NGN) может создавать существенные проблемы при разработке функционально совместимых протоколов;

c) основное беспокойство телекоммуникационных организаций вызывает возможность компрометации безопасности, ведущая к простою сети, который может быть очень дорогостоящим с точки зрения отношений с клиентами, упущенной выгоды и расходов на восстановление. Умышленные атаки, нацеленные на доступность национальной телекоммуникационной инфраструктуры, могут рассматриваться как проблема национальной безопасности;

d) системы и сети управления телекоммуникациями уязвимы для проникновений хакеров. Обычной мотивацией таких проникновений является хищение телекоммуникационных услуг. Такое хищение может быть спроектировано различными способами, такими как активирование диагностических функций, манипулирование учетными записями, изменение предоставления баз данных и перехват вызовов абонентов;

e) организации, предоставляющие услуги связи, помимо внешних проникновений озабочены компрометацией безопасности из внутренних источников, таких как, например, изменения конфигураций и баз данных сетевого менеджмента со стороны неуполномоченного персонала. Они могут быть случайными или намеренными.

С целью обеспечения защиты информационных активов в телекоммуникационной сфере, берущих начало из разных источников в разной телекоммуникационной среде, необходимы рекомендации по безопасности для

телекоммуникаций, чтобы поддерживать реализацию менеджмента информационной безопасности в телекоммуникационных организациях.

Эти рекомендации по безопасности должны применяться к:

a) телекоммуникационным организациям, стремящимся к преимуществу в бизнесе в результате реализации СМИБ;

b) телекоммуникационным организациям, стремящимся к достижению уверенности в том, что требования информационной безопасности заинтересованных сторон (например, их поставщиков, клиентов, регулятивных органов) будут выполнены;

c) пользователям и поставщикам продуктов и услуг, связанных с обеспечением информационной безопасности, для телекоммуникационной индустрии;

d) внутренним или внешним по отношению к телекоммуникационным организациям лицам, которые проводят оценку и аудит СМИБ на предмет ее соответствия требованиям ИСО/МЭК 27001;

e) внутренним или внешним по отношению к телекоммуникационным организациям лицам, которые проводят консультации или тренинг по СМИБ.

4.2.3 Информационные активы, требующие защиты

Организации для создания менеджмента информационной безопасности необходимо уточнить и идентифицировать все активы организации. Уточнение атрибутов и значимости активов позволяет реализовать соответствующие меры и средства контроля и управления.

Информация об активах, которые необходимо защищать в телекоммуникационных организациях может быть найдена в 7.1.1 «Инвентаризация активов».

4.2.4 Установление менеджмента информационной безопасности

4.2.4.1 Как устанавливать требования безопасности

Телекоммуникационным организациям необходимо установить свои требования безопасности. Существует три следующих основных источника требований безопасности:

a) результаты оценки рисков для поставщика телекоммуникационных услуг, с учетом его общей стратегии бизнеса и целей. Посредством оценки риска происходит

идентификация угроз для активов, оценка уязвимостей и вероятности возникновения угроз и приблизительная оценка их потенциального влияния;

b) правовые, законодательные, нормативные и договорные требования, которым должны соответствовать телекоммуникационные организации, и социально-культурная среда. Примерами законодательных требований для телекоммуникационных организаций служат неразглашение информации о соединениях (A.15.1.7) и обеспечение важнейших коммуникаций (A.15.1.8). Примерами социально-культурных требований являются обеспечение целостности сообщений, переданных, ретранслированных или полученных любым способом, доступности проводных или беспроводных телекоммуникационных средств для уполномоченных лиц и не причинения вреда другим телекоммуникационным средствам;

c) определенная совокупность принципов, целей и требований бизнеса для обработки информации, которую поставщик телекоммуникационных услуг разработал для поддержки своих операций.

4.2.4.2 **Оценка рисков безопасности**

Требования безопасности идентифицируются путем регулярной оценки рисков безопасности. Затраты на меры и средства контроля и управления должны сопоставляться с ущербом для бизнеса, возможным вследствие сбоев в обеспечении безопасности. Результаты оценки рисков помогут направить и определить соответствующие управленческие меры и приоритеты для менеджмента рисков информационной безопасности, а также реализовать меры и средства контроля и управления, выбранные для защиты от этих рисков.

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

4.2.4.3 **Выбор мер и средств контроля и управления**

После идентификации требований безопасности и оценки рисков и принятия решений по обработке рисков следует реализовать соответствующие меры контроля и управления для обеспечения уверенности в снижении рисков до допустимого уровня.

Настоящее руководство в дополнение к общему руководству по менеджменту информационной безопасности предоставляет дополнительные рекомендации и характерные для телекоммуникаций меры и средства контроля и управления с учетом требований, характерных для телекоммуникаций. Поэтому

телекоммуникационным организациям рекомендуется выбирать и реализовывать меры и средства контроля и управления из данного руководства. Кроме того, для удовлетворения особых потребностей в соответствующих случаях могут быть разработаны новые меры и средства контроля и управления.

Выбор мер и средств контроля и управления безопасностью зависит от решений организации, основанных на критериях принятия рисков, вариантах обработки рисков и общем подходе к менеджменту рисков, применимом к телекоммуникационным организациям, а также должны учитываться все соответствующие национальные и международные законодательные и нормативные акты.

4.2.4.4 **Важнейшие факторы успеха**.

Применять 0.7 стандарта ИСО/МЭК 27002.

5 Политика безопасности

Применять раздел 5 стандарта ИСО/МЭК 27002.

6 Организационные аспекты информационной безопасности

6.1 Задачи, решаемые внутри организации

Цель: Осуществлять менеджмент информационной безопасности в рамках организации.

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

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

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

точки контакта при обработке инцидентов информационной безопасности. Следует поощрять многопрофильный подход к обеспечению информационной безопасности.

6.1.1 Обязательства руководства по отношению к информационной безопасности

Применять 6.1.1 стандарта ИСО/МЭК 27002.

6.1.2 Координация вопросов информационной безопасности

Применять 6.1.2 стандарта ИСО/МЭК 27002.

6.1.3 Распределение обязанностей по обеспечению информационной безопасности

Применять 6.1.3 стандарта ИСО/МЭК 27002.

6.1.4 Процесс получения разрешения на использование средств обработки информации

Применять 6.1.4 стандарта ИСО/МЭК 27002.

6.1.5 Соглашения о конфиденциальности

Мера и средство контроля и управления

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

Рекомендация по реализации

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

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

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

c) необходимые действия при окончании срока действия соглашения;

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

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

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

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

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

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

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

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

Соглашения о конфиденциальности и неразглашении должны соответствовать всем применимым законам и нормам, под юрисдикцию которых они подпадают (см. также 15.1.1 в ИСО/МЭК 27002).

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

Рекомендация по реализации, характерная для телекоммуникаций

Для идентификации требований в отношении соглашений о конфиденциальности или неразглашении телекоммуникационные организации должны рассмотреть необходимость защиты для обеспечения неразглашения переданной информации:

a) наличия;

b) содержания;

c) источника;

d) адреса назначения; и

e) даты и времени

Дополнительная информация

Соглашения о конфиденциальности и неразглашении защищают информацию организации, а также информируют лиц, подписавших соглашение, об их

обязанности защищать, использовать и разглашать информацию внушающим доверие и санкционированным способом.

При различных обстоятельствах организации может потребоваться использование различных форм соглашений о конфиденциальности или неразглашении.

6.1.6 Контакт с различными инстанциями

Мера и средство контроля и управления

Должны поддерживаться соответствующие контакты с различными инстанциями.

Рекомендация по реализации

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

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

Рекомендация по реализации, характерная для телекоммуникаций

Если телекоммуникационные организации получают запросы от правоохранительных или следственных органов относительно информации, связанной с пользователями телекоммуникационных услуг, то эти телекоммуникационные организации нуждаются в подтверждении, что запросы прошли легитимные процессы и процедуры в соответствии с национальными законами и нормами.

Дополнительная информация

При осуществлении таких контактов может потребоваться поддержка процесса менеджмента инцидентов информационной безопасности (подраздел 13.2) или процесса планирования непрерывности бизнеса и действий в чрезвычайных ситуациях (раздел 14). Контакты с регулирующими органами также полезны для прогнозирования и подготовки к предстоящим изменениям в законах или нормах, которые должны соблюдаться организацией. Контакты с другими инстанциями включают контакты с коммунальными службами, скорой помощью и службами

охраны труда, провайдерами телекоммуникационных услуг (в связи с трассировкой линий связи и их доступностью).

6.1.7 Контакт со специализированными профессиональными группами

Применять 6.1.7 стандарта ИСО/МЭК 27002.

6.1.8 Независимая проверка информационной безопасности

Применять 6.1.8 стандарта ИСО/МЭК 27002.

6.2 Аспекты взаимодействия со сторонними организациями

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

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

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

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

6.2.1 Идентификация рисков, являющихся следствием работы со сторонними организациями

Применять 6.2.1 стандарта ИСО/МЭК 27002.

6.2.2 Рассмотрение вопросов безопасности при работе с клиентами

Мера и средство контроля и управления

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

Рекомендация по реализации

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

a) защита активов, включая:

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

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

3) целостность;

4) ограничения на копирование и разглашение информации;

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

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

d) политика управления доступом, охватывающая:

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

2) процесс авторизации в отношении доступа и привилегий пользователей;

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

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

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

f) описание каждой предоставляемой услуги;

g) определение необходимого и неприемлемого уровня обслуживания;

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

i) соответствующие обязательства организации и клиента;

j) обязательства относительно юридических вопросов, и способ обеспечения уверенности в соответствии правовым нормам, например, законодательству о защите данных, особенно с учетом различных требований национальных правовых систем, если договор предполагает сотрудничество с клиентами в других странах (см. также 15.1 в ИСО/МЭК 27002);

k) соблюдение прав на интеллектуальную собственность и авторских прав (см. 15.1.2 в ИСО/МЭК 27002), а также обеспечение правовой защиты любой совместной работы (см. также 6.1.5).

Рекомендация по реализации, характерная для телекоммуникаций

Прежде чем предоставлять клиентам доступ к каким-либо активам организации телекоммуникационные организации должны учитывать следующие условия при рассмотрении вопросов безопасности:

a) четкое соглашение относительно возможного повреждения или снижения качества телекоммуникационного канала обслуживания или других телекоммуникационных соединений, обеспечивающих работу пользователей;

b) четкое разграничение обязанностей между телекоммуникационными организациями, предоставляющими средства для телекоммуникационных услуг, и пользователями телекоммуникационных услуг;

c) четкий перечень возможных приостановок телекоммуникационных услуг в случае возникновения риска, например, угрозы спама, препятствующего непрерывному предоставлению телекоммуникационных услуг.

Дополнительная информация

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

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

6.2.3 Рассмотрение требований безопасности в договорах с третьей стороной

Мера и средство контроля и управления

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

Рекомендация по реализации

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

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

a) политика информационной безопасности;

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

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

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

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

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

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

6) конфиденциальность, целостность, доступность и любое другое значимое свойство (см. 2.5 в ИСО/МЭК 27002) активов;

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

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

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

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

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

g) четкая структура подотчетности и согласованные форматы представления отчетов;

h) ясный и определенный процесс менеджмента изменений;

i) политика управления доступом, охватывающая:

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

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

3) процесс авторизации в отношении доступа и привилегий пользователей;

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

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

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

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

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

l) определение необходимого и неприемлемого уровня обслуживания;

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

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

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

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

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

r) соответствующие обязательства сторон в рамках соглашения;

s) обязательства относительно юридических вопросов, и способов обеспечения уверенности в соответствии правовым требованиям, например, законодательству о защите данных, особенно с учетом различных требований национальных правовых систем, если договор предполагает сотрудничество с клиентами в других странах (см. 15.1 в ИСО/МЭК 27002);

t) соблюдение прав на интеллектуальную собственность и авторских прав (см. 15.1.2 в ИСО/МЭК 27002), а также обеспечение правовой защиты любой совместной работы (см. также 6.1.5);

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

v) условия перезаключения/окончания договоров:

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

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

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

Рекомендация по реализации, характерная для телекоммуникаций

Телекоммуникационные организации должны рассмотреть следующие условия на предмет их включения в договор с целью удовлетворения установленных требований безопасности:

a) четкая формулировка, касающаяся защиты от повреждения или ухудшения телекоммуникационного канала обслуживания или других телекоммуникационных соединений пользователей с использованием оборудования других телекоммуникационных организаций;

b) четкое разграничение обязанностей между телекоммуникационными организациями в отношении собственных средств телекоммуникационных услуг и средств других организаций.

Дополнительная информация

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

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

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

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

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

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

7 Менеджмент активов

7.1 Ответственность за активы

Цель: Обеспечить соответствующую защиту активов организации.

Все активы должны быть учтены и должны иметь назначенного владельца.

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

7.1.1 Инвентаризация активов

Мера и средство контроля и управления

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

Рекомендация по реализации

Организация должна идентифицировать все активы и документально оформлять значимость этих активов. Опись активов должна содержать всю информацию, необходимую для восстановления после бедствия, включая тип актива, формат, местоположение, информацию о резервных копиях, информацию о лицензировании и ценности для бизнеса. Опись не должна без необходимости

дублировать другие описи, но следует обеспечивать уверенность в том, что ее содержание выверено.

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

Рекомендация по реализации, характерная для телекоммуникаций

При разработке и поддержке описи активов должны быть точно определены и документально оформлены четкие обязанности в отношении собственных телекоммуникационных средств организации и средств других связанных или дочерних телекоммуникационных организаций.

Список активов должен быть всеобъемлющим и охватывать все имеющие ценность телекоммуникационные активы, включая информационные активы для сетевого оборудования, сетевых услуг и прикладных программ.

Дополнительные источники можно найти в «Библиографии».

Дополнительная информация

Существует много типов активов, включающих:

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

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

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

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

e) персонал, его квалификация, навыки и опыт;

f) нематериальные ценности, например, репутация и имидж организации.

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

Дополнительная информация для телекоммуникаций

Активы, относящиеся к телекоммуникационным организациям, включают много типов активов, таких как:

a) информация – данные о соединении, данные таблиц маршрутизации, информация об абонентах, данные «черного списка», информация о зарегистрированных услугах, эксплуатационная информация, информация о неисправностях, конфигурационная информация, информация о клиентах, платежная информация, шаблоны клиентских запросов, географическое местонахождение клиентов, статистические данные о трафиках, договоры и соглашения, системная документация, исследовательская информация, руководства пользователя, учебные материалы, методики эксплуатации или поддержки, планы обеспечения непрерывности бизнеса, мероприятия восстановления в плане действий в чрезвычайных ситуациях, записи аудита и архивированная информация;

b) программные активы – программные средства управления связью, программные средства менеджмента операций, программные средства управления информацией об абонентах, платежные программные средства, прикладные программные средства, системные программные средства, инструментальные средства разработки и утилиты;

c) физические активы – коммутаторы, кабели, терминальное оборудование, компьютерное оборудование (например, серверы и персональные компьютеры/рабочие станции), сменные носители данных и другое оборудование;

d) услуги – услуги стационарной телефонной связи, услуги мобильной телефонной связи, услуги асимметричной цифровой абонентской линии/оптической абонентской линии, услуги выделенной/коммутируемой линии, услуги подключения к Интернету, услуги информационного центра, услуги кабельного телевидения, услуги предоставления контента, услуги по аренде прикладных программ и клиентские услуги, включая платежные услуги и услуги центра обработки вызовов;

e) помещения и система поддерживающих услуг – строения, электрооборудование, системы кондиционирования воздуха, средства пожаротушения;

f) персонал – персонал по работе с клиентами, инженеры по телекоммуникационным системам, персонал, осуществляющий поддержку информационных технологий (ИТ), и персонал, связанный с поставщиками услуг третьей стороны;

g) нематериальные активы – управление организацией, ноу-хау, репутация и имидж организации.

7.1.2 Владение активами

Применять 7.1.2 стандарта ИСО/МЭК 27002.

7.1.3 Приемлемое использование активов

Применять 7.1.3 стандарта ИСО/МЭК 27002.

7.2 Классификация информации

Цель: Обеспечить уверенность в защищенности информации на надлежащем уровне.

Информацию следует классифицировать для определения ее необходимости, приоритетов и предполагаемой степени защиты при обработке информации. Предлагаемый вариант изменил смысл

Информация имеет различные степени чувствительности и критичности. Некоторые элементы могут потребовать дополнительного уровня защиты или специальной обработки. Схема классификации информации должна использоваться, чтобы определить соответствующее множество уровней защиты и установить связь с необходимостью принятия специальных мер обработки.

7.2.1 Рекомендации по классификации

Мера и средство контроля и управления

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

Рекомендация по реализации

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

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

В обязанности владельца актива (см. 7.1.2) входит классификация актива, ее периодический пересмотр и обеспечение уверенности в том, что она поддерживается на актуальном и соответствующем уровне. В отношении классификации следует учитывать эффект накопления, указанный в 10.7.2 в ИСО/МЭК 27002.

Предметом рассмотрения должно стать количество классификационных категорий и преимущества, получаемые от их использования. Чрезмерно сложные схемы могут стать обременительными и неоправданно дорогими для применения, или могут оказаться неосуществимыми. Следует проявлять осторожность в интерпретации классификационных меток на документах из других организаций, так как одни и те же метки могут иметь различный смысл.

Рекомендация по реализации, характерная для телекоммуникаций

При классификации информации, в дополнение к общим требованиям в отношении чувствительной и критичной информации организации, телекоммуникационные организации должны также учитывать следующее:

a) возможную потребность раздельной классификации информации, связанной с неразглашением информации о соединениях с точки зрения наличия, содержания, источника, адреса назначения, даты и времени переданной информации (см. А.15.1.7);

b) различие между важнейшими коммуникациями, требующими приоритетной обработки в случае чрезвычайной ситуации или риска чрезвычайной ситуации, и второстепенными коммуникациями (см. А.15.1.8).

Дополнительная информация

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

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

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

В общем, классификация информации – кратчайший путь для определения того, как эта информация должна быть обработана и защищена.

7.2.2 Маркировка и обработка информации

Применять 7.2.2 стандарта ИСО/МЭК 27002.

8 Безопасность, связанная с персоналом

8.1 Перед трудоустройством[1)]

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

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

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

Следует осуществлять соответствующую проверку всех кандидатов на должность, подрядчиков и представителей третьей стороны, особенно если работа связана с секретностью.

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

8.1.1 Роли и обязанности

Мера и средство контроля и управления

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

Рекомендация по реализации

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

a) реализации и действия в соответствии с политикой информационной безопасности организации (см. 5.1 в ИСО/МЭК 27002);

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

c) выполнения определенных процессов, связанных с безопасностью;

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

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

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

Рекомендация по реализации, характерная для телекоммуникаций

Телекоммуникационные организации должны назначить специалистов по телекоммуникациям и другой персонал, обладающий необходимыми полномочиями или соответствующими знаниями и навыками, которые будут контролировать вопросы, связанные с установкой, обслуживанием и эксплуатацией телекоммуникационных средств для телекоммуникационного бизнеса.

Соответствующие специалисты по телекоммуникационным системам и другой персонал должны быть извещены о порученных им ролях и обязанностях.

Дополнительная информация

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

8.1.2 Предварительная проверка

Мера и средство контроля и управления

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

Рекомендация по реализации

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

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

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

c) подтверждение заявленного образования и профессиональной квалификации;

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

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

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

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

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

Информацию обо всех рассматриваемых кандидатах, претендующих на занятие должностей в рамках организации, следует собирать и обрабатывать согласно любому применимому законодательству, действующему в соответствующей юрисдикции. В зависимости от применимого законодательства, данные кандидаты должны быть предварительно проинформированы о деятельностях, связанных с предварительными проверками.

Рекомендация по реализации, характерная для телекоммуникаций

Телекоммуникационные организации должны также дополнительно рассмотреть вопрос проведения более детальной проверки кандидатов на должности, дающие сотрудникам доступ к системам, критическим для предоставления услуг, к информации, связанной с законным доступом и законным прослушиванием линии связи, а также доступ, например, к информации о клиентах и содержанию вызовов клиентов.

8.1.3 Условия занятости

Мера и средство контроля и управления

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

Рекомендация по реализации

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

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

b) правовую ответственность и права сотрудников, подрядчиков и любых других клиентов, например, в части законов об авторском праве или законодательства о защите персональных данных (см. также 15.1.1 и 15.1.2 в ИСО/МЭК 27002);

c) обязанности в отношении классификации информации и менеджмента активов организации, связанных с информационными системами и услугами, выполняются сотрудником, подрядчиком или представителем третьей стороны (см. также 7.2.1 и 10.7.3 в ИСО/МЭК 27002);

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

e) ответственность организации за обработку персональной информации, включая персональную информацию, полученную в результате или в процессе работы в организации (см. также 15.1.4 в ИСО/МЭК 27002);

f) ответственность, распространяющуюся также и на работу вне помещений организации и в нерабочее время, например, в случае исполнения работы на дому (см. также 9.2.5 и 11.7.4 в ИСО/МЭК 27002);

g) действия, которые должны быть предприняты в случае, если сотрудник, подрядчик или представитель третьей стороны игнорирует требования безопасности организации (см. 8.2.3 в ИСО/МЭК 27002).

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

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

Рекомендация по реализации, характерная для телекоммуникаций

Правовая ответственность и права, связанные с неразглашением информации о соединениях и важнейшими коммуникациями, которые следует учитывать телекоммуникационным организациям, включены в законодательные и нормативные акты (см. А.15.1.7 и А.15.1.8).

Телекоммуникационные организации в условиях занятости должны прояснить и сформулировать ответственность за поддержку услуг связи, предоставляемых телекоммуникационными организациями.

Телекоммуникационные организации должны обеспечить уверенность в том, что любое лицо, участвующее в предоставлении телекоммуникационных услуг, хорошо осведомлено и осознает необходимость хранить секреты других людей, которые могли стать ему известны во время его профессиональной деятельности, связанной с телекоммуникационными услугами, и сохранять конфиденциальность даже после окончания работы в организации.

Дополнительная информация

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

8.2 В течение занятости

Применять 8.2 стандарта ИСО/МЭК 27002.

8.3 Прекращение или смена занятости

Применять 8.3 стандарта ИСО/МЭК 27002.

9 Физическая безопасность и защита от воздействий окружающей среды

9.1 Зоны безопасности

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

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

Уровень защищенности должен быть соразмерен выявленным рискам.

9.1.1 Периметр зоны безопасности

Мера и средство контроля и управления

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

Рекомендация по реализации

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

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

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

заперты, и внешняя защита должна быть предусмотрена для окон, особенно если они находятся на уровне земли;

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

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

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

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

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

Рекомендация по реализации, характерная для телекоммуникаций

Телекоммуникационные организации должны учитывать и реализовывать, при необходимости, следующие рекомендации относительно физических периметров безопасности:

a) центры телекоммуникационных операций должны быть оснащены соответствующими системами обнаружения физических вторжений;

b) оборудование для телекоммуникационных услуг, например, средства передачи данных, коммутационное оборудование и телекоммуникационная инфраструктура, должны быть физически отделены и расположены удаленно от

других средств, например, клиентских средств в управляемых информационных центрах;

c) физические барьеры должны быть установлены эффективно согласно неукоснительно соблюдаемой местной политике безопасности для обеспечения уверенности в защите корпоративных активов в любой момент времени, если физический барьер работает неисправно или политика не соблюдается, необходимо, чтобы этот вопрос незамедлительно решался руководством с соответствующим уровнем ответственности.

Дополнительная информация

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

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

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

9.1.2 Меры и средства контроля и управления физическим входом

Мера и средство контроля и управления

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

Рекомендация по реализации

Следует принимать во внимание следующие рекомендации:

a) дату и время входа и выхода посетителей следует регистрировать, и всех посетителей необходимо сопровождать, или они должны обладать соответствующим допуском; доступ следует предоставлять только для выполнения определенных авторизованных задач, а также необходимо инструктировать посетителей на предмет требований безопасности, и действий в случае аварийных ситуаций;

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

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

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

e) права доступа в зоны безопасности следует регулярно анализировать, пересматривать, и аннулировать при необходимости (см. 8.3.3 в ИСО/МЭК 27002).

Рекомендация по реализации, характерная для телекоммуникаций

Телекоммуникационные организации должны рассматривать следующие рекомендации:

a) операционные залы и центры управления телекоммуникационными средствами должны быть защищены с помощью соответствующих жестких мер и средств контроля и управления доступом в помещение;

b) на пропускном пункте информация о других посетителях должна быть защищена от несанкционированного доступа или просмотра, например, запись о дате и времени входа и выхода посетителя; работник пропускного пункта также должен проверять вещи посетителей при входе и выходе, чтобы воспрепятствовать вносу опасных объектов в помещения или выносу активов без разрешения.

9.1.3 Безопасность зданий, производственных помещений и оборудования

Применять 9.1.3 стандарта ИСО/МЭК 27002.

9.1.4 Защита от внешних угроз и угроз со стороны окружающей среды

Применять 9.1.4 стандарта ИСО/МЭК 27002.

9.1.5 Работа в зонах безопасности

Применять 9.1.5 стандарта ИСО/МЭК 27002.

9.1.6 Зоны общего доступа, приемки и отгрузки

Применять 9.1.6 стандарта ИСО/МЭК 27002.

9.2 Безопасность оборудования

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

Оборудование необходимо защищать от физических угроз и воздействия окружающей среды.

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

9.2.1 Размещение и защита оборудования

Мера и средство контроля и управления

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

Рекомендация по реализации

Необходимо рассмотреть следующие рекомендации по защите оборудования:

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

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

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

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

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

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

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

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

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

Рекомендация по реализации, характерная для телекоммуникаций

Если комплексы телекоммуникационных средств нескольких организаций размещены в одном и том же информационном центре, то телекоммуникационные организации должны реализовать соответствующие меры для защиты информации о клиентах, хранящейся в их комплексах. Такие комплексы должны быть физически отделены друг от друга, например, должны размещаться на разных этажах или в разных комнатах.

9.2.2 Поддерживающие услуги

Мера и средство контроля и управления

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

Рекомендация по реализации

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

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

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

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

необходимость установки системы сигнализации для обнаружения неправильного функционирования объектов поддерживающих услуг.

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

Рекомендация по реализации, характерная для телекоммуникаций

Желательно, чтобы средства энергоснабжения в изолированной зоне, например, мобильных базовых станциях, обеспечивали бесперебойное электропитание для всей нагрузки с возможностью выдержать перебои в работе основного источника питания в течение возможных перебоев. Если это невозможно, должен быть установлен механизм для обеспечения бесперебойного электропитания критического оборудования. Аккумуляторы могут требовать оснащения персональным электрогенератором, особенно в изолированных зонах.

Дополнительная информация

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

Дополнительная информация для телекоммуникаций

Телекоммуникационные организации должны определить в соглашениях необходимость надлежащего обслуживания и постоянного предоставления поддерживающих услуг, чтобы обеспечивать бесперебойное предоставление телекоммуникационных услуг.

9.2.3 Безопасность кабельной сети

Применять 9.2.3 стандарта ИСО/МЭК 27002.

9.2.4 Техническое обслуживание оборудования

Применять 9.2.4 стандарта ИСО/МЭК 27002.

9.2.5 Безопасность оборудования вне помещений организации

Применять 9.2.5 стандарта ИСО/МЭК 27002.

9.2.6 Безопасная утилизация или повторное использование оборудования

Применять 9.2.6 стандарта ИСО/МЭК 27002.

9.2.7 Перемещение имущества

Применять 9.2.7 стандарта ИСО/МЭК 27002.

10 Менеджмент коммуникаций и работ

10.1 Эксплуатационные процедуры и обязанности

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

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

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

10.1.1 Документальное оформление эксплуатационных процедур

Мера и средство контроля и управления

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

Рекомендация по реализации

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

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

а) обработку и управление информацией;

b) резервирование (см. 10.5);

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

d) инструкции по обработке ошибок или других исключительных ситуаций, которые могли бы возникнуть в процессе выполнения работы, включая ограничения на использование системных утилит (см. 11.5.4 в ИСО/МЭК 27002);

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

f) специальные инструкции по управлению выводом данных и обращению с носителями информации, например, использование специальной бумаги для печатающих устройств или управление выводом конфиденциальных данных, включая процедуры по безопасной утилизации выходных данных в случае сбоев в работе (см. 10.7.2 и 10.7.3 в ИСО/МЭК 27002);

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

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

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

Рекомендация по реализации, характерная для телекоммуникаций

Телекоммуникационные организации должны определить в эксплуатационных процедурах условия, при которых активируются процедуры обработки инцидентов, непредвиденных ситуаций или кризисов (см. 13.2).

10.1.2 Управление изменениями

Мера и средство контроля и управления

Изменения в конфигурации средств обработки информации и системах должны контролироваться.

Рекомендация по реализации

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

В частности, необходимо рассмотреть следующие аспекты:

a) определение и регистрацию существенных изменений;

b) планирование и тестирование изменений;

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

d) формализованную процедуру утверждения предполагаемых изменений;

e) подробное информирование об изменениях всех заинтересованных лиц;

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

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

Рекомендация по реализации, характерная для телекоммуникаций

Телекоммуникационные организации должны рассмотреть процедуры и записи для установки, перемещения и ликвидации средств.

Дополнительная информация

Неадекватный контроль изменений средств и систем обработки информации – распространенная причина системных сбоев и инцидентов безопасности. Изменения эксплуатационной среды, особенно при переходе от стадии разработки к стадии эксплуатации, могут оказывать влияние на надежность прикладных программ (см. 12.5.1 в ИСО/МЭК 27002).

Изменения эксплуатируемых систем следует проводить только в том случае, если на это имеется обоснованная причина, затрагивающая бизнес, например, возрастание риска в отношении системы. Обновление систем новейшими версиями эксплуатируемой системы или прикладных программ не всегда отвечает интересам бизнеса, поскольку оно может привнести большее число уязви
нестабильность, чем действующая версия. Могут также потребоваться

дополнительное обучение, расходы на лицензирование, поддержка, сопровождение и административный надзор, а также аппаратные средства, особенно в течение периода миграции.

10.1.3 Разделение обязанностей

Применять 10.1.3 стандарта ИСО/МЭК 27002.

10.1.4 Разделение средств разработки, тестирования и эксплуатации

Мера и средство контроля и управления

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

Рекомендация по реализации

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

Необходимо рассмотреть следующие вопросы:

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

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

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

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

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

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

Рекомендация по реализации, характерная для телекоммуникаций

В телекоммуникационных организациях содержание данных, используемых в среде тестирования и разработки, должно быть достаточным для тестирования системы и услуги в контексте реальных телекоммуникаций. Если тестовые данные включают чувствительную информацию (например, персональную информацию и записи о телефонных соединениях), то должны реализовываться соответствующие меры и средства контроля и управления, чтобы избежать непреднамеренной утечки информации, вызванной ошибками в программе или эксплуатационными ошибками.

Кроме того, должно осуществляться соответствующее управление тестовыми данными с учетом жизненного цикла данных, как например сбор эксплуатационных данных, включающих чувствительную информацию, формирование тестовых данных из эксплуатационных данных и уничтожение тестовых данных после тестирования.

Осуществляющий разработку персонал может пользоваться эксплуатационным паролям только тогда, когда имеются меры и средства (контроля и управления) выпуска паролей, поддерживающие эксплуатацию систем. Меры и средства контроля и управления должны обеспечивать изменение таких паролей после использования.

Дополнительная информация

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

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

Разработчики и специалисты, проводящие тестирование, могут также быть причиной угроз конфиденциальности эксплуатационной информации. Кроме того, если разработка и тестирование производятся в одной компьютерной среде, это

может стать причиной непреднамеренных изменений программного обеспечения или информации. Разделение средств разработки, тестирования и эксплуатации является, следовательно, целесообразным для уменьшения риска случайного изменения или неавторизованного доступа к программному обеспечению и данным бизнеса среды эксплуатации (см. также 12.4.2 на предмет защиты тестовых данных)

10.2 Менеджмент оказания услуг третьей стороной

Применять 10.2 стандарта ИСО/МЭК 27002.

10.3 Планирование и приемка систем

Применять 10.3 стандарта ИСО/МЭК 27002.

10.4 Защита от вредоносной и мобильной программы

Цель: Защита целостности программного обеспечения и информации.

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

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

10.4.1 Меры и средства контроля и управления против вредоносной программы

Применять 10.4.1 стандарта ИСО/МЭК 27002.

10.4.2 Меры и средства контроля и управления против мобильной программы

Мера и средство контроля и управления

Там, где разрешено использование мобильной программы, конфигурация должна обеспечивать уверенность в том, что разрешенная мобильная программа

функционирует в соответствии с ясно сформулированной политикой безопасности, а исполнение неразрешенной мобильной программы будет запрещено.

Рекомендация по реализации

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

a) обеспечивать выполнение действий мобильной программой в логически изолированной среде;

b) блокировать любое несанкционированное пользование мобильной программы;

c) блокировать прием мобильной программы;

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

e) контролировать ресурсы доступные мобильной программе;

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

Дополнительная информация

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

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

Дополнительная информация для телекоммуникаций

Некоторые примеры мобильной программы включают встроенные скрипты, ActiveX® и Java™. Поскольку мобильные программы связаны с рядом услуг промежуточного технологического программного обеспечения, в дополнение к общим мерам и средствам контроля и управления, направленным против вредоносных программ должны быть рассмотрены меры и средства контроля и

управления применительно к промежуточному технологическому программному обеспечению.

10.5 Резервирование

Применять 10.5 стандарта ИСО/МЭК 27002.

10.6 Менеджмент безопасности сети

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

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

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

10.6.1 Меры и средства контроля и управления сетями

Применять 10.6.1 стандарта ИСО/МЭК 27002.

Дополнительная рекомендация по реализации приведена в Приложении В (справочном).

10.6.2 Безопасность сетевых услуг

Мера и средство контроля и управления

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

Рекомендация по реализации

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

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

Дополнительная информация

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

Средствами обеспечения безопасности сетевых услуг могут быть:

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

b) технические параметры, требуемые для безопасного подключения сетевых услуг в соответствии с правилами безопасности сетевых соединений;

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

Дополнительная информация для телекоммуникаций

Для телекоммуникационных организаций обеспечение безопасности услуг, предоставляемых пользователям сети, включает следующее:

a) обеспечение безопасности OAM&P, а также конфигурирования сетевых услуг;

b) обеспечение безопасности управляющей и сигнальной информации, используемой сетевыми услугами (например, SIP для услуг VoIP);

c) защита данных и голоса конечного пользователя при использовании им сетевой услуги (например, трафика VoIP).

10.7 Обращение с носителями информации

Применять 10.7 стандарта ИСО/МЭК 27002.

10.8 Обмен информацией

Применять 10.8 стандарта ИСО/МЭК 27002.

10.9 Услуги электронной торговли

Применять 10.9 стандарта ИСО/МЭК 27002.

10.10 Мониторинг

Цель: Обнаружение неавторизованных действий, связанных с обработкой информации.

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

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

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

10.10.1 Контрольная регистрация

Мера и средство контроля и управления

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

Рекомендация по реализации

Контрольные журналы должны включать, при необходимости:

a) идентификаторы пользователей;

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

c) идентичность и местоположение терминала, если это возможно;

d) регистрацию успешных и отклоненных попыток доступа к системе;

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

f) изменения конфигурации системы;

g) использование привилегий;

h) использование системных утилит и прикладных программ;

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

j) сетевые адреса и протоколы;

k) сигналы тревоги, подаваемые системой управления доступом;

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

Рекомендация по реализации, характерная для телекоммуникаций

Телекоммуникационные организации должны установить соответствующее время хранения телекоммуникационных данных (например, учета используемых ресурсов, платежей, реагирования на жалобы, защиты от злоупотребления и законного доступа соответствующих инстанций) и незамедлительно удалить данные по истечении времени хранения или по достижении целей. Это должно осуществляться в соответствии с любыми применимыми требованиями бизнеса, правовыми и нормативными требованиями.

Дополнительная информация

Контрольные журналы могут содержать данные о вторжениях и конфиденциальные личные данные. Необходимо принимать соответствующие меры для защиты приватности (см. также 15.1.4 в ИСО/МЭК 27002). При возможности системным администраторам следует запрещать стирать или деактивировать журналы регистрации их собственных действий (см. 10.1.3).

Дополнительная информация для телекоммуникаций

Должны быть приняты соответствующие меры для обеспечения неразглашения информации о соединениях (см. А.15.1.7).

10.10.2 Использование системы мониторинга

Применять 10.10.2 стандарта ИСО/МЭК 27002.

10.10.3 Защита информации журналов регистрации

Применять 10.10.3 стандарта ИСО/МЭК 27002.

10.10.4 Журналы регистрации администратора и оператора

Применяется 10.10.4 стандарта ИСО/МЭК 27002.

10.10.5 Регистрация неисправностей

Применять 10.10.5 стандарта ИСО/МЭК 27002.

10.10.6 Синхронизация часов

Применять 10.10.6 стандарта ИСО/МЭК 27002.

11 Управление доступом

11.1 Требования бизнеса по управлению доступом

Цель: Управлять доступом к информации.

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

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

11.1.1 Политика управления доступом

Мера и средство контроля и управления

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

Рекомендация по реализации

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

Необходимо, чтобы в политике было учтено следующее:

а) требования в отношении безопасности конкретных прикладных программ бизнеса;

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

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

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

e) соответствующие требования законодательства и любые договорные обязательства в отношении защиты доступа к данным или услугам (см. 15.1 в ИСО/МЭК 27002);

f) стандартные профили доступа пользователей для должностных ролей в организации;

g) менеджмент прав доступа в распределенной среде или сетях с учетом всех типов доступных соединений;

h) разделение ролей в отношении управления доступом, например, запрос доступа, авторизация доступа, администрирование доступа;

i) требования в отношении формального разрешения запросов доступа (см. 11.2.1 в ИСО/МЭК 27002);

j) требования в отношении периодического пересмотра управления доступом (см. 11.2.4 в ИСО/МЭК 27002);

k) аннулирование прав доступа (см. 8.3.3 в ИСО/МЭК 27002).

Рекомендация по реализации, характерная для телекоммуникаций

Телекоммуникационные организации должны определить соответствующие правила управления доступом к оборудованию, расположенному в помещениях пользователей. Доступ должен быть основан на владении информацией, а не на владении физическими активами. Например, только пользователь телекоммуникационного оборудования должен иметь доступ к адресной книге, хранящейся в мобильном телефоне, но не иметь доступа к любой информации, относящейся к структуре системы, такой как идентификатор терминала.

Дополнительная информация

При определении правил управления доступом, следует принимать во внимание следующее:

a) различие между правилами, обязательными для исполнения, и рекомендациями, которые являются необязательными или обусловленными чем-либо;

b) установление правил, основанных на предпосылке «все в общем случае запрещено, пока явно не разрешено», а не на более слабом принципе «все в общем случае разрешено, пока явно не запрещено»;

c) изменения в информационных метках (см. 7.2), инициированных как автоматически средствами обработки информации, так и по усмотрению пользователя;

d) изменения в правах пользователя как устанавливаемые автоматически информационной системой, так и определенные администратором;

e) правила, которые требуют особого разрешения перед применением, а также те, которые не требуют разрешения.

Правила управления доступом должны поддерживаться формальными процедурами и четко определенными обязанностями (см. например, 6.1.3, 11.3, 10.4.1, 11.6 в ИСО/МЭК 27002).

11.2 Менеджмент доступа пользователей

Применять 11.2 стандарта ИСО/МЭК 27002.

11.3 Обязанности пользователя

Применять 11.3 стандарта ИСО/МЭК 27002.

11.4 Управление доступом к сети

Применять 11.4 стандарта ИСО/МЭК 27002.

11.5 Управление доступом к эксплуатируемой системе

Применять 11.5 стандарта ИСО/МЭК 27002.

11.6 Управление доступом к информации и прикладным программам

Применимы 11.6 стандарта ИСО/МЭК 27002.

11.7 Мобильная вычислительная техника и дистанционная работа

Применять 11.7 стандарта ИСО/МЭК 27002.

12 Приобретение, разработка и эксплуатация информационных систем

12.1 Требования к безопасности информационных систем

Применять 12.1 стандарта ИСО/МЭК 27002.

12.2 Корректная обработка в прикладных программах

Применять 12.2 стандарта ИСО/МЭК 27002.

12.3 Криптографические меры и средства контроля и управления

Применять 12.3 стандарта ИСО/МЭК 27002.

12.4 Безопасность системных файлов

Цель: Обеспечить уверенность в безопасности системных файлов.

Доступ к системным файлам и исходным текстам программ следует контролировать, а проекты ИТ и деятельности по их поддержке необходимо осуществлять безопасным образом. Необходимо проявлять осторожность в среде тестирования, чтобы не подвергать риску чувствительную информацию.

12.4.1 Управление эксплуатируемым программным обеспечением

Мера и средство контроля и управления

Необходимо применять процедуры контроля установки программного обеспечения в эксплуатируемых системах.

Рекомендация по реализации

Чтобы свести к минимуму риск повреждения эксплуатируемых систем, необходимо учесть следующие рекомендации в отношении контроля изменений:

a) обновление эксплуатируемого программного обеспечения, прикладных программ и библиотек программ, должны выполнять только обученные администраторы при наличии соответствующего разрешения руководства (см. 12.4.3);

b) эксплуатируемые системы должны содержать только утвержденный исполняемый программный код, и не должны содержать коды разработки или компиляторы;

c) прикладные программы и программное обеспечение следует внедрять в эксплуатируемую систему только после всестороннего и успешного тестирования, которое должно выполняться на изолированных системах и включать в себя тесты на пригодность к эксплуатации, безопасность, влияние на другие системы и удобство для пользователя (см. также 10.1.4); необходимо обеспечивать уверенность в том, что все соответствующие библиотеки исходных текстов программ были обновлены;

d) меры и средства контроля и управления конфигурацией системы необходимо использовать согласно системной документации для сохранения управления всем реализуемым программным обеспечением;

e) прежде чем изменения будут реализованы, необходимо применять метод отката;

f) в контрольном журнале должны быть сохранены все обновления эксплуатируемой библиотеки программ;

g) предыдущие версии прикладного программного обеспечения следует сохранять на случай непредвиденных обстоятельств;

h) старые версии программного обеспечения следует архивировать вместе со всей требуемой информацией и параметрами, процедурами, конфигурационными деталями и поддерживающим программным обеспечением, до тех пор, пока данные хранятся в архиве.

Необходимо, чтобы поставляемое поставщиком программное обеспечение, используемое в действующей системе, поддерживалось на уровне, обеспечиваемом поставщиком. Со временем поставщики программного обеспечения прекращают поддерживать более старые версии программного обеспечения. Организация

должна учитывать риски, когда она полагается на неподдерживаемое программное обеспечение.

Любое решение об обновлении программного обеспечения до новой версии должно учитывать требования бизнеса в отношении изменения и безопасности новой версии, т. е., введение новых функциональных возможностей безопасности или количество и серьезность проблем безопасности, связанных с этой версией. Исправления (патчи) программного обеспечения следует применять, если они помогают удалять или снижать уязвимости безопасности (см. 12.6.1 в ИСО/МЭК 27002).

Физический или логический доступ следует предоставлять поставщикам только для целей поддержки, по мере необходимости и на основании разрешения руководства. Действия поставщика должны подвергаться мониторингу.

Программное обеспечение компьютеров может использовать поставляемые внешним (иностранным) поставщиком программное обеспечение и модули, которые должны быть контролируемы и управляемы во избежание несанкционированных изменений, которые могут способствовать нарушению безопасности.

Рекомендация по реализации, характерная для телекоммуникаций

Телекоммуникационные организации должны сводить к минимуму риск повреждения находящихся в эксплуатации систем, учитывая следующие рекомендации по контролю за изменениями:

a) если прикладные программы и операционное программное обеспечение должны быть установлены на чувствительных системах, таких как коммутационный комплексы, то следует провести тестирование с полным охватом маршрута;

b) если прикладное программное обеспечение является чувствительным, то следует сохранять, по крайней мере, три поколения программного обеспечения.

Дополнительная информация

Эксплуатируемую систему следует обновлять только при необходимости, например, если текущая версия эксплуатируемой системы больше не удовлетворяет требованиям бизнеса. Обновления не следует проводить только потому, что доступна новая версия для эксплуатируемой системы. Новые версии систем, находящихся в промышленной эксплуатации, могут быть менее безопасными, менее стойкими и менее понятными, чем текущие системы.

12.4.2 Защита тестовых данных системы

Применять 12.4.2 стандарта ИСО/МЭК 27002.

12.4.3 Управление доступом к исходным текстам программ

Применять 12.4.3 стандарта ИСО/МЭК 27002.

12.5 Безопасность в процессах разработки и поддержки

Применять 12.5 стандарта ИСО/МЭК 27002.

12.6 Менеджмент технических уязвимостей

Применять 12.6 стандарта ИСО/МЭК 27002.

13 Менеджмент инцидентов информационной безопасности

13.1 Оповещение о событиях и уязвимостях информационной безопасности

Цель: Обеспечить уверенность в том, что о событиях и уязвимостях информационной безопасности оповещается способом, который позволяет своевременно предпринять корректирующее действие.

Необходимо использовать формальные процедуры информирования и эскалации[1)]. Все сотрудники, подрядчики и представители третьей стороны должны быть осведомлены о процедурах информирования о различных типах событий и уязвимостях, которые могли бы оказать негативное влияние на безопасность активов организации. Они должны незамедлительно сообщать о любых событиях и уязвимостях информационной безопасности определенному контактному лицу.

13.1.1 Оповещение о событиях информационной безопасности

Мера и средство контроля и управления

О событиях информационной безопасности необходимо незамедлительно сообщать через соответствующие каналы управления.

[1)] В контексте менеджмента инцидентов информационной безопасности под термином «процедуры эскалации» понимается передача расследования инцидента на более высокий уровень в случае невозможности проведения адекватного расследования на более низком уровне (примечание редактора).

Рекомендация по реализации

Необходимо внедрить формальную процедуру оповещения о событиях информационной безопасности, вместе с процедурой реагирования и эскалации инцидента, в которой излагается действие, необходимое при получении сообщения о событии информационной безопасности. Должна быть установлена «точка контакта» для уведомления о событиях информационной безопасности. Необходимо обеспечить уверенность в том, что эта «точка контакта» известна в организации, всегда доступна и способна к адекватному и своевременному реагированию.

Все сотрудники, подрядчики и представители третьей стороны должны быть осведомлены о своей обязанности незамедлительно сообщать о любых событиях информационной безопасности. Они должны быть также осведомлены о процедуре информирования о событиях информационной безопасности и «точке контакта». Необходимо, чтобы процедуры информирования включали:

a) соответствующие процессы обратной связи, для обеспечения уверенности в том, что сотрудник, сообщивший о событиях информационной безопасности, был уведомлен о результатах, после того, как проблема была решена и закрыта;

b) формы сообщений о событиях информационной безопасности, чтобы помочь информирующему лицу обеспечить соответствующие действия, которые необходимо совершить в случае, если произойдет событие информационной безопасности;

c) правила поведения в случае, если произойдет событие информационной безопасности, а именно:

1) сразу же обращать внимание на все важные детали (например, тип несоответствия или недостатка, возникшие неисправности, сообщения на экране, странное поведение системы);

2) не предпринимать самостоятельно никакого действия, а немедленно сообщить в «точку контакта»;

d) ссылку на установленные формальные дисциплинарные процессы относительно сотрудников, подрядчиков и пользователей третьей стороны, которые нарушаю правила безопасности.

Среда с высоким уровнем риска может быть оснащена сигнализацией о принуждении[1)], с помощью которой лица, на которые оказывается давление, могут указать на такие проблемы. Процедура реагирования на сигнализацию о принуждении должна отражать место высокого риска, которое показывает сигнализация.

Рекомендация по реализации, характерная для телекоммуникаций

Для сотрудничества с группой реагирования на инциденты должна существовать «точка контакта», подготовленная для оценки, реагирования и извлечения уроков из инцидентов безопасности. В телекоммуникационных организациях такой пункт может быть создан виртуально. Группа реагирования на инциденты должна быть уполномочена принимать незамедлительные решения о способах обработки инцидента. Кроме того, должны быть установлены взаимосвязи между группой реагирования и внешними сторонами (например, группой реагирования на компьютерные инциденты – CERT, правоохранительными организациями, аварийными службами, клиентами и партнерами по бизнесу).

При необходимости телекоммуникационные организации должны быстро сообщать об инцидентах своим клиентам с помощью сообщений по электронной почте и/или предоставленной им Web-страницы.

Дополнительная информация

Примерами событий и инцидентов, связанных с нарушением информационной безопасности, могут быть:

a) потеря услуг, оборудования или средств обслуживания;

b) неисправности в системе или перегрузки;

c) ошибки оператора;

d) несоблюдение политики или рекомендаций;

e) нарушения мер физической безопасности;

f) неконтролируемые изменения систем;

g) программный или аппаратный сбой;

h) нарушения доступа.

Обращая должное внимание на аспекты конфиденциальности, можно для повышения осведомленности пользователей использовать инциденты

[1)] Сигнализация о принуждении – это способ, с помощью которого можно незаметно показать, что действие совершается «под принуждением».

информационной безопасности (см. 8.2.2 в ИСО/МЭК 27002) в качестве примеров того, что могло бы произойти, как реагировать на такие инциденты и как избежать их в будущем. Чтобы иметь возможность должным образом рассмотреть события и инциденты информационной безопасности, необходимо собирать свидетельства как можно быстрее после происшествия (см. 13.2.3).

Неисправная работа или другое аномальное поведение системы может служить показателем атаки на безопасность или реального недостатка безопасности, поэтому о них следует сообщать как о событии информационной безопасности.

Дополнительную информацию относительно отчетности о событиях информационной безопасности и о менеджменте инцидентов информационной безопасности можно найти в ИСО/МЭК ТО 18044.

13.1.2 Оповещение об уязвимостях безопасности

Применяется 13.1.2 стандарта ИСО/МЭК 27002.

13.2 Менеджмент инцидентов информационной безопасности и необходимое совершенствование

Цель: Обеспечить уверенность в том, что в отношении менеджмента инцидентов информационной безопасности применяется последовательный и эффективный подход.

Обязанности должностных лиц обработки событий и уязвимостей информационной безопасности должны осуществляться эффективным образом, если о них было сообщено, хотя бы один раз. Процесс непрерывного совершенствования необходимо применять в отношении реагирования на общий менеджмент инцидентов информационной безопасности, а также их мониторинг и оценку.

Если нужны доказательства нарушения информационной безопасности, их следует собрать, чтобы обеспечить уверенность в соответствии законодательным требованиям.

13.2.1 Обязанности и процедуры

Мера и средство контроля и управления

Необходимо устанавливать обязанности должностных лиц по осуществлению менеджмента и процедуры для обеспечения быстрого, эффективного и должного реагирования на инциденты информационной безопасности.

Рекомендация по реализации

В дополнение к информированию о событиях и недостатках информационной безопасности (см. 13.1), необходимо также использовать мониторинг систем, сигналов тревоги и уязвимостей для обнаружения инцидентов информационной безопасности (см. 10.10.2). В отношении процедур менеджмента инцидентов информационной безопасности необходимо учитывать следующие рекомендации:

a) необходимо установить процедуры обработки различных типов инцидентов информационной безопасности, включая:

1) сбои информационных систем и потерю обслуживания;

2) вредоносные программы (см. 10.4.1);

3) отказ в обслуживании;

4) ошибки, являющиеся следствием неполноты или неточности данных бизнеса;

5) нарушения конфиденциальности и целостности;

6) неправильное использование информационных систем;

b) в дополнение к обычным планам обеспечения непрерывности бизнеса (см. 14.1.3), процедуры должны также охватывать (см. также 13.2.2):

1) анализ и выявление причины инцидента;

2) ограничение распространения последствий;

3) планирование и реализацию корректирующего действия для предотвращения повторения, если это необходимо;

4) взаимодействие с теми, кто испытал влияние инцидента или участвовал в восстановлении после инцидента;

5) сообщение о предпринятом действии в соответствующий орган;

c) контрольные записи и аналогичные доказательства необходимо собирать (см. 13.2.3) и защищать соответствующим образом, для:

1) анализа внутренних проблем;

2) использования в качестве судебного доказательства в отношении возможного нарушения договора или нормативного требования, а также в случае гражданского или уголовного производства, например, на основании неправильного использования компьютера или законодательства о защите данных;

3) обсуждения условий о выплате компенсации поставщиками программного обеспечения и услуг;

d) действия по восстановлению после проявления недостатков безопасности и по устранению сбоев систем следует тщательно контролировать; процедуры должны обеспечивать уверенность в том, что:

1) только четко идентифицированному и уполномоченному персоналу разрешен доступ к эксплуатируемым системам и данным (см. также 6.2 на предмет внешнего доступа);

2) все предпринятые аварийные действия документируются в деталях;

3) руководство информируется об аварийном действии, и такое действие анализируется должным образом;

4) целостность систем, а также мер и средств контроля и управления бизнеса подтверждается с минимальной задержкой.

Цели менеджмента инцидентов информационной безопасности следует согласовать с руководством, а также необходимо обеспечить уверенность в том, что лица, ответственные за осуществление менеджмента инцидентов информационной безопасности, понимают приоритеты организации по обработке таких инцидентов.

Рекомендация по реализации, характерная для телекоммуникаций

Если согласованный уровень услуг больше не выполняется, телекоммуникационные организации должны осуществить эскалацию любых инициированных клиентами вопросов, затрагивающих клиентов и служащих относительно функционирования существующих конфигураций объектов, таких как выход из строя аппаратных средств, сетевые проблемы и групповых конфигураций.

Все клиенты должны быть полностью проинформированы о процедурах эскалации проблем и иметь соответствующую доступную документацию.

Например, инициированные клиентами вопросы могут быть расставлены в соответствии с приоритетами на основе представленных критериев:

a) клиентский пункт полностью не работает или не отвечает требованиям соглашений об уровне услуг;

b) клиентский пункт серьезно затронут нарушением: одна или несколько систем не работают, или имеется существенные потери и (или) задержка пакетов;

c) ухудшение обслуживания клиентов;

d) запросы клиентов.

Телекоммуникационные организации, ответственные за предоставление телекоммуникационных услуг в качестве важной утилиты, должны установить механизмы и (или) процедуры для сдерживания и ликвидации инцидентов информационной безопасности и восстановления после них, а также точного и своевременного обнаружения и анализа инцидентов, возникающих в телекоммуникационных системах.

Такие механизмы и (или) процедуры должны включать следующие действия:

a) анализ индикации и взаимосвязанной информации с целью установления факта наличия инцидента;

b) классификация и определение приоритета инцидента в соответствии с планом менеджмента инцидентов;

c) сообщение об инциденте соответствующему персоналу организации и внешним организациям;

d) сбор, сохранение, защита и документирование свидетельств;

e) если возможно, изолирование телекоммуникационной системы и прекращение ее использования; если система должна быть подвергнута проверке, то её необходимо отсоединить от любых телекоммуникационных сетей до ее повторного включения;

f) ликвидация инцидента путем выявления и уменьшения всех использованных им уязвимостей и устранения вредоносного программного обеспечения, несоответствующих материалов и других компонентов;

g) восстановление после инцидента с подтверждением нормального функционирования всех затронутых систем; при необходимости реализация дополнительного мониторинга для слежения за будущей взаимосвязанной деятельностью.

Дополнительная информация

Инциденты информационной безопасности могут выходить за границы организаций и стран. В отношении реагирования на такие инциденты имеется растущая потребность в координации реагирования и совместном использовании информации об этих инцидентах с внешними организациями, при необходимости.

Дополнительная информация для телекоммуникаций

Телекоммуникационные организации должны обмениваться информацией об инцидентах информационной безопасности с соответствующими организациями, такими как Telecom-ISAC.

13.2.2 Извлечение уроков из инцидентов информационной безопасности

Мера и средство контроля и управления

Должны быть созданы механизмы, позволяющие установить типы, объемы и стоимость инцидентов информационной безопасности, которые должны быть измерены и проконтролированы.

Рекомендация по реализации

Информацию, полученную в результате оценки инцидентов информационной безопасности, следует использовать для идентификации повторяющихся или оказывающих значительное влияние инцидентов.

Рекомендация по реализации, характерная для телекоммуникаций

Телекоммуникационные организации должны установить механизмы и (или) процедуры для обмена накопленным опытом и совершенствования менеджмента инцидентов, учитывая следующие действия:

a) проведение совещания после инцидента, в повестку дня которого включаются усвоенные уроки; на совещании должны рассматриваться способы совершенствования мер безопасности и самого процесса обработки инцидентов;

b) сбор данных об инцидентах, таких как количество обработанных инцидентов, полное время на обработку, расходы и т. д., и использование их для совершенствования плана менеджмента инцидентов;

c) сохранение соответствующих доказательств, с учетом судебного преследования, законодательных/нормативных актов и расходов (см. 13.2.3).

Дополнительная информация

Оценка инцидентов информационной безопасности может указывать на необходимость совершенствования существующих или внедрения дополнительных

мер и средств контроля и управления, чтобы снизить частоту, ущерб и стоимость будущих происшествий, или должна быть принята во внимание при пересмотре политики безопасности (см. 5.1.2 в ИСО/МЭК 27002).

13.2.3 Сбор доказательств

Применять 13.2.3 стандарта ИСО/МЭК 27002.

14 Менеджмент непрерывности бизнеса

14.1 Аспекты информационной безопасностью в рамках менеджмента непрерывности бизнеса

Цель: Противодействовать прерываниям видов деятельности в рамках бизнеса организации и защищать важнейшие процессы бизнеса от последствий значительных сбоев информационных систем или чрезвычайных ситуаций и обеспечивать их своевременное возобновление.

Необходимо внедрить процесс менеджмента непрерывности бизнеса с целью минимизации негативного влияния на организацию и восстановление после потери информационных активов (которые могут быть результатом, например, стихийных бедствий, несчастных случаев, отказов оборудования и преднамеренных действий) до приемлемого уровня с помощью комбинирования профилактических и восстановительных мер и средств контроля и управления. Указанный процесс должен выявлять критические процессы бизнеса и объединять требования к менеджменту информационной безопасности в части непрерывности бизнеса с другими требованиями непрерывности, касающихся таких вопросов, как функционирование, кадровое обеспечение, складское хозяйство, транспорт и оборудование.

Последствия стихийных бедствий, нарушений безопасности, отказов в обслуживании и потери доступности обслуживания необходимо анализировать на предмет их влияния на бизнес. Необходимо разработать и внедрить планы обеспечения непрерывности бизнеса с целью обеспечения уверенности в том, что значимые операции могут быть возобновлены в течение требуемого времени. Информационная безопасность должна стать составной частью всего процесса обеспечения непрерывности бизнеса и других процессов менеджмента, реализуемых в организации.

Необходимо, чтобы менеджмент непрерывности бизнеса включал в себя меры и средства контроля и управления по выявлению и снижению рисков в дополнение к общему процессу оценки рисков, ограничения последствий разрушительных инцидентов и обеспечения уверенности в том, что информация, требуемая для процессов бизнеса, легко доступна.

14.1.1 Включение информационной безопасности в процесс менеджмента непрерывности бизнеса

Мера и средство контроля и управления

Следует разрабатывать и поддерживать управляемый процесс для обеспечения непрерывности бизнеса во всей организации, который учитывает требования к информационной безопасности, необходимые для обеспечения непрерывности бизнеса организации.

Рекомендация по реализации

Данный процесс должен объединять следующие ключевые элементы менеджмента непрерывности бизнеса:

a) понимание рисков, с которыми сталкивается организация, с точки зрения вероятности и продолжительности воздействия, включая определение критических процессов бизнеса и установление их приоритетов (см. 14.1.2);

b) определение всех активов, вовлеченных в критические процессы бизнеса (см. 7.1.1);

c) понимание последствий для бизнеса, которые могут быть вызваны прерываниями, обусловленными инцидентами информационной безопасности (важно, чтобы были найдены решения, которые будут применяться как в случае незначительных, так и существенных инцидентов, потенциально угрожающих жизнедеятельности организации), а также определение целей бизнеса применительно к средствам обработки информации;

d) рассмотрение возможности подходящего страхования, которое может стать частью общего процесса непрерывности бизнеса, а также частью менеджмента эксплуатационного риска;

e) определение и рассмотрение внедрения дополнительных превентивных и нейтрализующих мер и средств контроля и управления;

f) определение достаточности финансовых, организационных, технических ресурсов и ресурсов окружающей среды для реагирования на выявленные требования информационной безопасности;

g) обеспечение безопасности персонала и защита средств обработки информации и имущества организации;

h) разработку и документальное оформление планов обеспечения непрерывности бизнеса, учитывающих требования информационной безопасности в соответствии с согласованной стратегией обеспечения непрерывности бизнеса (см. 14.1.3);

i) регулярное тестирование и обновление данных планов и применяемых процессов (см. 14.1.5);

j) обеспечение уверенности в том, что менеджмент непрерывности бизнеса органично вписывается в процессы и структуру организации; ответственность за процесс менеджмента информационной безопасности следует назначать на соответствующем уровне в рамках организации (см. 6.1.1).

Рекомендация по реализации, характерная для телекоммуникаций

Телекоммуникационные организации должны обеспечивать уверенность в безопасности телекоммуникационных средств, т. е. в их соответствии требованиям информационной безопасности как в одном из основных элементов менеджмента непрерывности бизнеса.

14.1.2 Непрерывность бизнеса и оценка риска

Применять 14.1.2 стандарта ИСО/МЭК 27002.

14.1.3 Разработка и внедрение планов обеспечения непрерывности бизнеса, учитывающих информационную безопасность

Мера и средство контроля и управления

Следует разработать и внедрить планы обеспечения непрерывности бизнеса с целью поддержки или восстановления операций и обеспечения доступности информации на требуемом уровне и в требуемые сроки после прерывания или сбоя критических процессов бизнеса.

Рекомендация по реализации

Процесс планирования непрерывности бизнеса должен предусматривать следующее:

a) определение и согласование всех обязанностей и процедур, связанных с обеспечением непрерывности бизнеса;

b) определение приемлемых потерь информации и услуг;

c) внедрение процедур, позволяющих восстановить и возобновить операции бизнеса и доступность информации в требуемые сроки; особое внимание следует уделить оценке внешних и внутренних зависимостей бизнеса и существующих договоров;

d) эксплуатационные процедуры, которым необходимо следовать в ожидании завершения восстановления и возобновления процесса;

e) документальное оформление согласованных процедур и процессов;

f) соответствующее обучение сотрудников согласованным процедурам и процессам, включая управление в критических ситуациях;

g) тестирование и обновление планов.

Необходимо, чтобы в процессе планирования особое внимание было обращено на требуемые цели бизнеса, например, восстановление определенных услуг связи для клиентов в приемлемые сроки. Следует учитывать потребность в необходимых для этого услугах и ресурсах, включая укомплектованность персоналом, ресурсы, не связанные с обработкой информации, а также меры по переходу на аварийный режим средств обработки информации. Такие меры по переходу на аварийный режим могут включать в себя договоренности с третьей стороной в виде взаимных соглашений или коммерческих абонируемых услуг.

Планы обеспечения непрерывности бизнеса должны учитывать уязвимости организации и поэтому могут содержать чувствительную информацию, нуждающуюся в соответствующей защите. Копии планов обеспечения непрерывности бизнеса следует хранить на достаточном расстоянии от основного здания, чтобы Руководство должно обеспечить уверенность в том, что обновление и защита планов обеспечения непрерывности бизнеса осуществляется на том же уровне, что и в основном здании. Другие материалы, необходимые для выполнения планов по обеспечению непрерывности бизнеса, следует также хранить в удаленном месте.

, то

уровень реализуемых мер и средств контроля и управления безопасности в таких помещениях должен равняться уровню мер, реализуемых в основном здании.

Рекомендация по реализации, характерная для телекоммуникаций

При разработке и внедрении плана обеспечения непрерывности бизнеса телекоммуникационные организации должны рассматривать возможность включения в него плана восстановления телекоммуникационных услуг и обеспечения уверенности клиентов телекоммуникационных услуг в важнейших коммуникациях при аварии. Если соседние строения или площадки повреждены или требуют эвакуации, средства телекоммуникационных услуг могут фактически стать неконтролируемыми, даже если сами средства не повреждены. Телекоммуникационные организации должны предусматривать меры по устранению таких ситуаций. ???

Дополнительная информация

Следует заметить, что планы по управлению в критических ситуациях и действия, (см. f в 14.1.3) могут отличаться от менеджмента непрерывности бизнеса; т. е., может случиться так, что кризис может быть улажен обычными процедурами управления.

14.1.4 Основы планирования непрерывности бизнеса

Применять 14.1.4 стандарта ИСО/МЭК 27002.

14.1.5 Тестирование, поддержка и пересмотр планов непрерывности бизнеса

Применять 14.1.5 стандарта ИСО/МЭК 27002.

15 Соответствие

Применять раздел 15 стандарта ИСО/МЭК 27002.

Приложение А
(обязательное)
Дополнительный перечень мер и средств контроля и управления для телекоммуникаций

В данном приложении представлены определения новых целей, новых мер и средств контроля и управления, а также новых рекомендаций по реализации в виде дополнительного перечня мер и средств контроля и управления для телекоммуникаций. Цели управления из ИСО/МЭК 27002, связанные с этими новыми мерами и средствами контроля и управления, повторяются без изменений. Любой организации, реализующей эти меры и средства контроля и управления в контексте СМИБ, предназначенной для соответствия ИСО/МЭК 27001, рекомендуется дополнить свою Ведомость применения мер и средств контроля и управления (сформированную на основе приложения А стандарта ИСО/МЭК 27001), включив туда меры и средства контроля и управления, указанные в данном приложении.

А.1 Физическая безопасность и защита от воздействий окружающей среды здесь и далее это не ошибка, а дополнение к соответствующему разделу/подразделу стандарта (см. заголовки)

А.1.1 Зоны безопасности

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

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

Уровень защищенности должен быть соразмерен выявленным рискам.

A.1.1.1 Защита узлов связи

Мера и средство контроля и управления

Для узлов связи, где размещаются телекоммуникационные средства, такие как коммутационное оборудование, должна проектироваться, разрабатываться и применяться физическая защита.

Рекомендация по реализации

Для защиты телекоммуникационных средств, таких как коммутационное оборудование, обеспечивающее телекоммуникационный бизнес (в дальнейшем называемых узлами связи) должны соблюдаться следующие условия:

a) для узлов связи должна быть выбрана площадка на твердой почве; в некоторых случаях может выбираться менее твердая почва при условии принятия адекватных мер для предотвращения неровной осадки;

b) для узлов связи должна быть выбрана площадка с окружающей средой наименее восприимчивой к повреждениям от ветра, воды и т. д.; в случаях выбора площадки с окружающей средой восприимчивой к повреждениям, должны быть приняты соответствующие меры для защиты от воздействия стихии;

c) для узлов связи должна быть выбрана площадка с окружающей средой наименее восприимчивой к повреждениям от сильного электромагнитного поля; в случаях выбора площадки, подверженной действию сильных электромагнитных полей, должны быть приняты соответствующие меры для защиты телекоммуникационных аппаратных с помощью электромагнитных экранов;

d) узлы связи не должны располагаться на площадках, расположенных рядом с сооружениями для хранения опасных веществ, несущих угрозу взрыва или воспламенения;

e) здания узлов связи должны иметь сейсмостойкую конструкцию;

f) здания узлов связи должны иметь огнестойкую или огнеупорную конструкцию;

g) здания узлов связи должны обладать соответствующей прочностью конструкции, удовлетворяющей необходимой нагрузке на перекрытия;

h) в узлах связи должна быть установлена автоматическая пожарная сигнализация.

A.1.1.2 Защита телекоммуникационных аппаратных

Мера и средство контроля и управления

Для аппаратных, где размещаются телекоммуникационные средства для обеспечения телекоммуникационного бизнеса, должна проектироваться, разрабатываться и применяться физическая защита.

Рекомендация по реализации

Для защиты помещений, где располагаются средства для предоставления телекоммуникационных услуг (в дальнейшем называемых телекоммуникационными аппаратными), должны рассматриваться следующие меры и средства контроля и управления:

a) телекоммуникационные аппаратные должны располагаться в местах, наименее уязвимых к внешнему воздействию, такому как природные бедствия;

b) телекоммуникационные аппаратные должны располагаться в местах, наименее уязвимых к вторжению неуполномоченного персонала; для предотвращения таких вторжений должны быть приняты адекватные меры;

c) телекоммуникационные аппаратные должны располагаться в местах, наименее уязвимых к затоплению; если они должны быть расположены в уязвимых к затоплению местах, то должны быть приняты необходимые меры, такие как поднятие уровня пола, установка водной преграды или специальных средств для отвода воды;

d) телекоммуникационные аппаратные должны располагаться в местах, наименее уязвимых к повреждениям от сильных электромагнитных полей; если они должны быть расположены в местах, подверженных влиянию сильных электромагнитных полей, то они должны быть защищены с помощью электромагнитных экранов или каких-то других мер; в случаях, когда в телекоммуникационных аппаратных установлены источники электропитания, должны быть приняты соответствующие меры для предупреждения помех от электромагнитного поля;

e) важнейшие средства должны размещаться исключительно в телекоммуникационных аппаратных с соответствующей физической защитой;

f) должны быть приняты меры для предотвращения разрушения и падения материалов, использованных для стен, пола, потолка и т. д., например, в связи с землетрясением с нормальной предсказуемой магнитудой;

g) материалы, использованные для пола, стен, потолка и т. д., должны быть негорючими или огнестойкими;

h) должны быть приняты меры для борьбы со статическим электричеством;

i) кабельные каналы, соединяющие телекоммуникационные аппаратные, должны быть спроектированы так, чтобы замедлять или предотвращать распространение огня;

j) при необходимости должны быть приняты меры для защиты от электромагнитного воздействия помещений, предназначенных для хранения данных, и сейфов с данными;

k) при необходимости должны быть приняты меры по обеспечению огнестойкости помещений для хранения данных и специальных хранилищ данных;

l) в телекоммуникационной аппаратной и в помещении с оборудованием для кондиционирования воздуха должна быть установлена автоматическая пожарная сигнализация;

m) в телекоммуникационной аппаратной и в помещении с оборудованием для кондиционирования воздуха должны быть установлены огнетушители;

n) в телекоммуникационной аппаратной должно обеспечиваться кондиционирование воздуха;

o) телекоммуникационная аппаратная, где размещаются важные средства связи, должна обеспечиваться системой кондиционирования воздуха, отдельной от той, что предназначена для офисов и других помещений.

A.1.1.3 Защита физически изолированных рабочих зон

Мера и средство контроля и управления

Для физически изолированных рабочих зон, где размещаются телекоммуникационные средства для обеспечения телекоммуникационного бизнеса, должны проектироваться, разрабатываться и реализовываться меры и средства контроля и управления физической безопасностью.

Рекомендация по реализации

Для защиты физически изолированной рабочей зоны (например, базовой станции мобильной связи), где располагаются телекоммуникационные средства для обеспечения телекоммуникационного бизнеса (в дальнейшем называемой изолированной рабочей зоной), должны быть рассмотрены следующие меры и средства контроля и управления:

a) изолированные рабочие зоны должны быть сейсмостойкими, отвечая обязательным национальным или региональным стандартам;

b) изолированные рабочие зоны должны быть оснащены автоматическими противопожарными системами;

c) изолированные рабочие зоны должны подвергаться дистанционному мониторингу с целью обнаружения сбоев оборудования, нарушения энергоснабжения, возгорания, контроля влажности, температуры и т. д.;

d) периметры физической безопасности должны быть обеспечены надлежащим образом, например, с использованием надежных ограждений, охватывающих изолированную рабочую зону; поскольку они обычно работают в автоматическом режиме, требуется оснащение их автоматической системой оповещения операционного центра в случае инцидента.

A.1.2 Безопасность мест, находящихся под контролем другой стороны

Цель: Обеспечивать защиту оборудования, размещенного вне помещений телекоммуникационной организации (например, совместное размещение) от физических угроз и угроз внешней среды.

A.1.2.1 Оборудование, размещенное в помещениях другой организации, предоставляющей услуги связи

Мера и средство контроля и управления

При установке оборудования вне собственных помещений, оборудование должно быть размещено в защищенных зонах, снижающих любые риски от угроз или опасностей со стороны внешней среды и от возможности несанкционированного доступа.

Рекомендация по реализации

Для защиты оборудования телекоммуникационной организации, размещенного в помещениях других телекоммуникационных организаций, должны обеспечиваться следующие меры и средства контроля и управления:

a) должны быть определены границы и взаимодействие с другой телекоммуникационной организацией, а оборудование должно легко изолировано от оборудования другой организации, если это потребуется;

b) должно быть заключено соглашение с другой телекоммуникационной организацией о поставке поддерживающих утилит;

c) руководство должно подтвердить, что место, где будет установлено оборудование, соответствует обеспечению желаемого уровня безопасности.

Дополнительная информация

Должны быть заранее проверены соглашение и правила, касающиеся достижения желаемого уровня безопасности с другими телекоммуникационными организациями, с целью согласования уровней безопасности помещений другой организации и собственных помещений телекоммуникационной организации.

A.1.2.2 Оборудование, размещенное в помещениях пользователей

Мера и средство контроля и управления

При установке оборудования телекоммуникационных организаций в помещениях клиента телекоммуникационных услуг для соединения с оборудованием клиента, должна обеспечиваться защита оборудования организации для снижения риска от угроз или опасностей внешней среды и от возможности несанкционированного доступа.

Рекомендация по реализации

Для защиты оборудования, размещенного на площадке клиента телекоммуникационных услуг, должны обеспечиваться следующие меры и средства контроля и управления:

a) оборудование, такое как, например, стойка для размещения аппаратуры, установленное на площадке клиента, должно быть прочным, чтобы его нельзя было легко открыть неуполномоченным пользователям;

b) должны быть определены граница взаимодействия с клиентом, и оборудование должно быть легко изолировано от оборудования клиента, если это потребуется;

c) должна быть возможность осуществления удаленного мониторинга состояния оборудования или управления оборудованием.

A.1.2.3 Взаимосвязанные телекоммуникационные услуги

Мера и средство контроля и управления

В случае предоставления взаимосвязанных телекоммуникационных услуг телекоммуникационные организации должны определить границу взаимодействия с другими телекоммуникационными организациями, чтобы можно было обеспечить быстрое разъединение и изоляцию каждой организации тогда, когда идентифицируется событие риска.

Рекомендация по реализации

Должны быть обеспечены соответствующие меры и средства контроля и управления, предназначенные для проверки услуг взаимодействующих телекоммуникационных организаций в плане проверки их реализации в условиях нормальной эксплуатации или нет.

Для диагностирования проблем и принятия корректирующих мер у организаций должна быть возможность изолировать свое оборудование от оборудования других организаций и заново подключить его в точке взаимного соединения.

Телекоммуникационные организации должны последовательно проводить мониторинг состояния трафика в точке взаимного соединения.

Телекоммуникационные организации должны определить в соглашении или договоре возможность прекращения предоставления телекоммуникационных услуг тем клиентам, чьи коммуникации представляют проблему для беспрепятственного взаимодействия телекоммуникационных организаций.

A.2 Менеджмент коммуникаций и работ

A.2.1 Менеджмент безопасности сети

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

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

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

A.2.1.1 Менеджмент безопасности поставки телекоммуникационных услуг

Мера и средство контроля и управления

Телекоммуникационные организации должны установить уровни безопасности для различных предложений бизнеса о предоставляемых телекоммуникационных услугах, известить о них клиентов до предоставления услуг и надлежащим образом поддерживать и осуществлять менеджмент своих телекоммуникационных услуг.

Рекомендация по реализации

Телекоммуникационные организации должны выполнять следующие функции для клиентов телекоммуникационных услуг:

a) предоставлять перечень и четкое изложение условий безопасности, уровней услуг и требований менеджмента телекоммуникационных услуг;

b) обеспечивать необходимое информирование с целью защиты пользователей телекоммуникационных услуг от спама, Интернет-преступлений, компьютерных вирусов и т. д.

Телекоммуникационные организации должны также предусмотреть:

c) реализацию отвечающих соответствующим законам и предписаниям мер и средств контроля и управления, таких как предупреждение несанкционированного перехвата и обеспечения взаимодействий с другими поставщиками телекоммуникационных услуг;

d) предоставление коммуникаций, необходимых для специальных уровней услуг, таких как важнейшие коммуникации в аварийных ситуациях (см. A.15.1.8);

e) реализацию мер и средств контроля и управления безопасностью для каждой предоставляемой услуги, подобных следующим:

- услуги IP соединений/услуги информационного центра:

  1) меры и средства контроля и управления против спама (см. A.10.6.4);

  2) меры и средства контроля и управления против DoS/DDoS-атаки (см. A.10.6.5);

  3) меры и средства контроля и управления против технических уязвимостей (см. 12.6.1 в ИСО/МЭК 27002);

- стационарная/мобильная телефонная связь:

  4) обработка важнейших коммуникаций;

  5) обеспечение приоритетных вызовов в чрезвычайной ситуации;

  6) меры и средства контроля и управления против перегрузки трафика телефонных вызовов;

- управляемые услуги:

  7) использование аутентификации/шифрования;

  8) тщательно спланированная обработка в привилегированном режиме;

f) реализацию мер и средств контроля и управления безопасностью для строгой поддержки следующих элементов управления информацией при поставке услуг:

1) обеспечение неразглашения информации о соединениях, включая детали телефонных вызовов;

2) защита персональной информации.

Для поддержки предоставляемых телекоммуникационных услуг телекоммуникационные организации должны применять следующие меры и средства контроля и управления:

g) соответствующее техническое обслуживание средств передачи данных, таких как кабели, и оперативный ремонт в аварийных ситуациях;

h) соответствующее техническое обслуживание коммутационного оборудования для телекоммуникационных услуг или постоянный мониторинг их информационной нагрузки; переключение на резервное оборудование или другие маршруты, чтобы избежать перегрузки трафика в чрезвычайных ситуациях;

i) методы и средства поддержки функций телекоммуникационных средств в случае DoS-атак, которые могут вынудить коммутационное оборудование, такое как маршрутизаторы, обрабатывать больший объем трафика по сравнению с обычными ситуациями;

j) соответствующий менеджмент маршрутной информации и управляющей информации, такой как DNS.

Дополнительная информация

При поставке телекоммуникационных услуг телекоммуникационные организации должны учитывать подробное описание этих услуг, чтобы избежать навязывания ложного представления об услугах посредством умышленного сокрытия отображения URL от пользователей телекоммуникационных услуг по несоответствующим причинам, и таких операций, из-за которых пользователям телекоммуникационных услуг придется приостанавливать или ослаблять функцию проверки безопасности на своем терминале.

A.2.1.2 Реагирование на спам

Мера и средство контроля и управления

Телекоммуникационные организации должны предусмотреть политику реагирования на спам и реализовать соответствующие меры и средства контроля и

управления для установления благоприятной и желательной среды для передачи сообщений по электронной почте.

Рекомендация по реализации

Если телекоммуникационные организации узнают о факте спама из жалобы пользователя телекоммуникационных услуг и о том, что соответствующим спамером является их собственный клиент, они должны обратиться к соответствующему клиенту с запросом о прекращении рассылки спама.

Если в ответ на такой запрос спамером не предпринимаются или не ожидаются соответствующие действия, то телекоммуникационные организации должны приостановить поставку телекоммуникационных услуг соответствующему клиенту, чтобы блокировать рассылку спама.

Если спам рассылается из сети других телекоммуникационных организаций, с которыми взаимодействуют телекоммуникационные средства данной организации, то она должна просить соответствующую организацию принять необходимые меры по блокированию спама, а соответствующая организация должна принять необходимые меры в ответ на такой запрос.

Для принятия эффективных мер против спама телекоммуникационные организации должны работать в тесном сотрудничестве с другими телекоммуникационными организациями, а также национальными и зарубежными организациями, занимающимися борьбой со спамом.

Телекоммуникационные организации должны разрабатывать и реализовывать политику, направленную против спама, в соответствии с национальными законами и нормами и делать их доступными для публики.

Дополнительная рекомендация по реализации приводится в Приложении В (справочном).

A.2.1.3 Реагирование на DoS/DDoS-атаки

Мера и средство контроля и управления

Телекоммуникационные организации должны предусмотреть политику реагирования на DoS/DDoS-атаки и реализовать соответствующие меры и средства контроля и управления для установления благоприятной и «комфортной» среды для телекоммуникационных услуг.

Рекомендация по реализации

Если телекоммуникационные организации узнают о случае DoS/DDoS-атак, они должны принять соответствующие контрмеры для того, чтобы обеспечить стабильное предоставление телекоммуникационных услуг.

Хотя конкретные необходимые меры зависят от вида DoS/DDoS-атак, телекоммуникационные организации должны учитывать следующие контрмеры:

a) фильтрация заголовков пакетов, направляемых на сайт, подвергшийся атаке;

b) введение ограничения для коммуникационного порта, используемого для DoS/DDoS-атак;

c) уменьшение или приостановление эксплуатации отдельных телекоммуникационных средств.

Если DoS/DDoS-атаку осуществляет собственный клиент телекоммуникационных организаций, то следует приостановить оказание телекоммуникационных услуг соответствующему клиенту, чтобы блокировать DoS/DDoS-атаки на телекоммуникационные средства.

Если DoS/DDoS-атаки исходят из сети других телекоммуникационных организаций, с которыми связаны телекоммуникационные средства данной организации, то она должна просить соответствующую организацию принять необходимые меры для блокирования DoS/DDoS-атак, а соответствующая организация должна принять необходимые меры в ответ на такой запрос.

Для принятия эффективных мер против DoS/DDoS-атак телекоммуникационные организации должны работать в тесном сотрудничестве с другими телекоммуникационных организациями, а также национальными и зарубежными организациями, занимающимися борьбой с кибер-терроризмом.

Дополнительная рекомендация по реализации приводится в Приложении В (справочном).

A.3 Управление доступом

A.3.1 Управление доступом к сети

Цель: Предотвратить неавторизованный доступ к сетевым услугам.

Доступ к внутренним и внешним сетевым услугам должен быть контролируемым.

Это необходимо для получения уверенности в том, что пользователи, которые имеют доступ к сетям и сетевым услугам, не нарушают их безопасность, путем:

a) обеспечения соответствующих интерфейсов между сетью организации и сетями, принадлежащими другим организациям, и общедоступными сетями;

b) внедрения соответствующих механизмов аутентификации в отношении пользователей и оборудования;

c) предписанного управления доступом пользователей к информационным услугам.

A.3.1.1 Идентификация и аутентификация пользователями поставщика телекоммуникационных услуг

Мера и средство контроля и управления

Телекоммуникационные организации должны обеспечить соответствующую меру и средство контроля и управления для пользователей, чтобы те могли идентифицировать и аутентифицировать телекоммуникационные организации.

Рекомендация по реализации

Если телекоммуникационные услуги используются через мобильную связь или посредством удаленного подключения (т. е. через оборудование других организаций), то существуют угрозы не обеспечения неразглашения информации о соединениях из-за имитации кем-либо роли посредника. Поэтому для пользователей телекоммуникаций должны быть обеспечены соответствующие меры и средства контроля и управления, чтобы они могли идентифицировать и аутентифицировать телекоммуникационные организации.

В случае, когда пользователи телекоммуникационных услуг не могут аутентифицировать телекоммуникационные организации, телекоммуникационные организации должны уведомлять пользователей о том, что функция аутентификации недоступна, вместе с возможными рисками, которым они подвергаются.

Дополнительная информация

Существует несколько альтернативных вариантов с использованием технологии шифрования для идентификации и аутентификации.

Одной из возможных атак в случае, когда пользователи не могут правильно идентифицировать и аутентифицировать телекоммуникационные организации, являются атаки «человек в середине».

A.4 Соответствие

A.4.1 Соответствие требованиям законодательства

Цель: Избежать нарушений любого закона, правовых, нормативных или договорных обязательств, а также любых требований безопасности.

Проектирование, функционирование, использование и управление информационных систем может быть предметом применения правовых, нормативных и договорных требований безопасности.

Следует консультироваться с юристами организации в отношении конкретных юридических вопросов, или с практикующими юристами, имеющими соответствующую квалификацию. Законодательные требования разных стран отличаются друг от друга, и они могут меняться в отношении информации, созданной в одной стране и переданной в другую страну (например, информационный поток, передаваемый через границу).

A.4.1.1 Неразглашение информации о соединениях

Мера и средство контроля и управления

Должно обеспечиваться неразглашение информации о соединениях, обрабатываемых телекоммуникационными организациями.

Рекомендация по реализации

Телекоммуникационные организации должны учитывать следующие рекомендации:

a) надлежащим образом обслуживать телекоммуникационные средства для обеспечения уверенности в неразглашении информации о соединениях;

b) принимать необходимые меры для предотвращения непреднамеренного разглашения информации о других соединениях во время обычного использования в точке подключения терминального оборудования пользователей телекоммуникационных услуг к телекоммуникационному каналу;

c) принимать необходимые меры для предотвращения несанкционированного доступа, уничтожения или фальсификации записей и данных пользователей телекоммуникационных услуг, хранящихся в телекоммуникационных средствах;

d) запрещать несанкционированное или незаконное использование персоналом телекоммуникационных организаций любой информации, связанной с соединениями клиентов;

e) установить соответствующий период хранения телекоммуникационных данных, в рамках временного периода, требуемого для выполнения задач, связанных с сохранением данных, и незамедлительное удаление их по истечении периода хранения или по достижении целей;

f) запретить предоставление каких-либо секретов о соединениях третьим сторонам, не имея законного основания или согласия самих пользователей телекоммуникационных услуг;

g) предложить функциональную возможность, посредством которой пользователи телекоммуникационных услуг могут в каждом конкретном случае принять решение, направлять или нет свой идентификатор (например, идентификатор вызывающего абонента) для обеспечения возможности выполнения услуги «идентификация вызывающего абонента»;

h) запретить предоставление идентификатора вызывающего абонента третьим сторонам, не имея законного основания или согласия самих пользователей телекоммуникационных услуг;

i) предложить клиентам телекоммуникационных услуг возможность выбора, заносить или нет их номера телефонов или идентификаторы в списки, связанные с другими услугами (в поддержку услуг «справочного стола»); если пользователи просят не заносить их номера в списки, то телекоммуникационные организации должны незамедлительно исключить их данные из услуг «справочного стола»;

j) если телекоммуникационные организации получают запросы о предоставлении информации, связанной с пользователями телекоммуникационных услуг, включая неразглашение информации о соединениях, то телекоммуникационные организации нуждаются в подтверждении, что запросы правоохранительных или следственных органов прошли легитимную процедуру в соответствии с национальными законами и нормативными актами.

A.4.1.2 Важнейшие коммуникации

Мера и средство контроля и управления

В случае стихийного бедствия, несчастного случая, другой чрезвычайной ситуации или риска их возникновения телекоммуникационные организации должны отдавать приоритет важнейшим коммуникациям, поддержание которых необходимо для предотвращения, помощи или восстановления при таких инцидентах, или для обеспечения безопасности перевозок, связи или энергоснабжения, а также для поддержания общественного порядка.

Рекомендация по реализации

Телекоммуникационные организации должны учитывать возможность приостановления или ограничения части своей телекоммуникационной деятельности с целью обеспечения важнейших коммуникаций, осуществляемых, например, приведенными ниже организациями и (или) в соответствии с национальными законами и нормативными актами:

a) метеорологическими организациям;

b) организациями по предотвращению затопления;

c) пожарными службами;

d) организациям по оказанию помощи в чрезвычайных ситуациях;

e) организациями, непосредственно связанными с охраной общественного порядка;

f) организациями, непосредственно связанными с обороной;

g) организациями, непосредственно связанными с безопасностью на море;

h) организациями, непосредственно связанными с обеспечением транспорта;

i) организациями, непосредственно связанными с услугами связи;

j) организациями, непосредственно связанными с энергоснабжением;

k) организациями, непосредственно связанными с водоснабжением;

l) организациями, непосредственно связанными с газоснабжением;

m) избирательными организациями;

n) журналистскими организациями;

o) финансовыми учреждениями;

p) медицинскими учреждениями;

q) организациями, непосредственно связанными с поставками продовольствия;

r) другими национальными или местными организациями, управляющими важнейшими коммуникациями.

Телекоммуникации организации в случае, когда их телекоммуникационные средства взаимодействуют с телекоммуникационными средствами других телекоммуникационных организаций, должны принять необходимые меры для заключения договора о приоритетном обслуживании важнейших коммуникаций, чтобы обеспечить уверенность в беспрепятственном и непрерывном функционировании важнейших коммуникаций.

A.4.1.3 Законность действий в чрезвычайных ситуациях

Мера и средство контроля и управления

Все меры, осуществляемые телекоммуникационными организациями в чрезвычайных ситуациях, должны ограничиваться мерами, необходимыми и достаточными для законной самообороны или экстренной эвакуации. Такие меры должны быть уместными и не чрезмерными.

Рекомендация по реализации

Телекоммуникационные организации должны заранее разработать процедуры на случай непредвиденных обстоятельств, включающих инциденты информационной безопасности, и получить советы и рекомендации от юристов по вопросам, не являются ли установленные чрезвычайные меры чрезмерными, и что они необходимы и достаточны для законной самообороны или экстренной эвакуации.

Телекоммуникационные организации должны ознакомить и информировать своих клиентов телекоммуникационных услуг о том, что организации могут нуждаться в принятии необходимых мер, таких как приостановка предоставления телекоммуникационных услуг, для реагирования на инциденты, например, когда соединение со средствами клиентов телекоммуникационных услуг мешает функционированию средств телекоммуникационных организаций или средств других клиентов телекоммуникационных услуг и других площадок, а также может оказывать влияние на защиту и безопасность людей.

Приложение В
(справочное)
Дополнительные рекомендации по реализации

В.1 Меры безопасности сети для защиты от кибератак

a) Защита сетевого оборудования

Телекоммуникационные средства должны быть надлежащим образом защищены, чтобы избежать существенных помех в предоставлении телекоммуникационных услуг, вызванных неожиданным поведением, которое может быть ненамеренно спровоцировано вредоносными программами, попавшими от пользователей телекоммуникационных услуг или телекоммуникационных средств других организаций.

Для защиты оборудования IP-сетей, такого как серверы и маршрутизаторы, от кибератак (например, DDoS-атак) у телекоммуникационных организаций должны быть механизмы фильтрации сообщений или ограничения полосы частот связи в IP-адресах, коммуникационных портах и прикладных протоколах, соответственно. В зависимости от телекоммуникационных услуг такие механизмы фильтрации должны реализовываться в связи с обработкой сигналов управления, аутентификацией пользователя, мерами и средствами контроля и управления доступом.

b) Меры, направленные против имитации источника

Телекоммуникационные организации должны реализовывать меры для защиты от имитации IP-адресов (IP спуфинг).

Для предотвращения имитации источника должны быть реализованы соответствующие меры и средства контроля и управления безопасностью для предотвращения несанкционированного доступа в системах, обеспечивающих аутентификацию пользователей, путем введения строгих мер и средств контроля и управления паролями, а также стойких функций аутентификации, например, обязательного использования паролей, не поддающихся предсказанию и длиной выше определенной, и введения одноразовых паролей и строгих аутентификационных токенов.

Телекоммуникационные средства, связанные с важнейшими коммуникациями, должны приводить в исполнение механизмы для предотвращения имитации идентификатора источника (вызывающего абонента). Например, рекомендуется введение терминалов на базе жестко закодированного идентификатора или механизмов

верификации идентификатора вызывающего абонента в телекоммуникационном сетевом оборудовании путем использования в момент регистрации и запроса соединения зарегистрированного пароля.

c) Привлечение внимания пользователей телекоммуникационных услуг

Для сдерживания непреднамеренных кибератак с инфицированных персональных компьютеров пользователей телекоммуникационных услуг или быстрого и надлежащего реагирования на кибератаки телекоммуникационные организации должны четко указывать сроки и условия предоставления услуг, а также информацию об ограничении использования телекоммуникационных услуг в случае перегрузки телекоммуникационных средств.

Телекоммуникационные организации должны обращать внимание пользователей телекоммуникационных услуг на такие угрозы, как вирусы и ботнеты, которые могут привести к кибератакам, и призывать их к принятию собственных необходимых мер.

Примечание – Термин «ботнет» обычно используется для упоминания группы скомпрометированных компьютеров (называемых компьютерами-зомби), запускающих программы, обычно называемые троянскими конями, червями или бэкдорами, в общей инфраструктуре контроля и управления. Инициатор ботнета («хозяин бота»), обычно действуя с неблаговидными целями, может удаленно управлять группой обычно с помощью таких средств, как Интернет-чат (IRC).

B.2 Меры безопасности сети для защиты от сетевой перегрузки

a) Механизмы обнаружения и ограничения сетевой перегрузки

У телекоммуникационных средств должны быть механизмы обнаружения сетевой перегрузки и избегания концентрации соединений в случае сетевой перегрузки.

Для телекоммуникационных средств, связанных с важнейшими коммуникациями, следует учитывать, что ограничение связи, такое как фильтрация сообщений, не вызывает побочных эффектов в непрерывном предоставлении важнейших коммуникаций.

Телекоммуникационные организации должны осознавать пределы эффективности соответствующих коммуникационных средств и реализовывать механизмы контроля числа запросов на предмет достижения предела. Кроме того, если это возможно, трафик должен обрабатываться распределенными средствами.

b) Заблаговременный сбор информации о событиях, которые могут вызывать перегрузку

Телекоммуникационными организациями должны быть предусмотрены правила работы по сбору информации, касающейся бедствий и планируемых мероприятий, которые могут вызвать перегрузку сети, например, установление структуры сбора метеосводок и информации о планируемых мероприятиях. Должны быть установлены механизмы и процедуры обобщения собранной информации, с целью поддержания информированности персонала.

c) Меры по улучшению временной пропускной способности

При необходимости, учитывая масштаб потенциальных разрушения и бедствий, должен рассматриваться вопрос использования распределенных центров обработки и ввода в эксплуатацию дополнительных средств, а также соответствующих изменений конфигурации.

d) Идентификация и приоритет важнейших коммуникаций

Важнейшим коммуникациям должно уделяться особое внимание.

В случаях, когда телекоммуникационные организации связаны с другими телекоммуникационными организациями, должно быть заключено соглашение о приоритетной обработке важнейших коммуникаций и приняты соответствующие приоритетные меры.

e) Заблаговременный сбор информации о событиях, которые могут инициировать сбои

Поскольку бедствия, несчастные случаи и социальные явления, как правило, являются причиной сбоев телекоммуникационных средств и перегрузок сети, телекоммуникационные организации должны заранее рассмотреть меры по сбору соответствующей информации и регулярному накоплению знаний.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 27001:2005	IDT	ГОСТ Р ИСО/МЭК 27001–2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
ИСО/МЭК 27002:2005	IDT	ГОСТ Р ИСО/МЭК 27002–2011 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»

Примечание – В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT – идентичные стандарты.

Библиография

ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications.*

ISO/IEC 18028-1:2006, *Information technology – Security techniques – IT network security – Part 1: Network security management (ИСО/МЭК 18028-1:2006 Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационной технологии. Часть 1. Менеджмент сетевой технологии)* *.

ISO/IEC 18028-2:2006, *Information technology – Security techniques – IT network security – Part 2: Network security architecture.*

ISO/IEC 18028-3:2005, *Information technology – Security techniques – IT network security – Part 3: Securing communications between networks using security gateways.*

ISO/IEC 18028-4:2005, *Information technology – Security techniques – IT network security – Part 4: Securing remote access.*

ISO/IEC 18028-5:2006, *Information technology – Security techniques – IT network security – Part 5: Securing communications across networks using virtual private networks.*

ISO/IEC 18043:2006, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems. (ИСО/МЭК 18043:2006 Информационные технологии. Методы защиты. Выбор, применение и операции систем обнаружения вторжения)* *.

ISO/IEC TR 18044:2004, *Information technology – Security techniques – Information security incident management.*

ISO/IEC 27005:2008, *Information technology – Security techniques – Information security risk management.*

---

* Официальный перевод этого международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

УДК 001.4:025.4:006.354 ОКС 35.040 Т 00
01.040.01

Ключевые слова: информационная технология, информационная безопасность, мера и средство контроля и управления, телекоммуникация, телекоммуникационная услуга, менеджмент информационной безопасности, менеджмент безопасности сети, физическая безопасность, управление доступом, менеджмент активов, менеджмент инцидентов, менеджмент непрерывности бизнеса

Подписано в печать 30.04.2014. Формат 60x84 1/8.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ФГУП «СТАНДАРТИНФОРМ»

123995 Москва, Гранатный пер., 4.

info@gostinfo.ru

gost.e-ecolog.ru gost.e-ecolog.ru