ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ГОСТ Р ИСО/МЭК 27002— 2021**

## Информационные технологии

# МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

## Свод норм и правил применения мер обеспечения информационной безопасности

**(ISO/IEC 27002:2013, IDT)**

Издание официальное

Москва
Стандартинформ
2021

## Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН), Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) и Акционерным обществом «Эшелон — Северо-Запад» (АО «Эшелон-СЗ») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 022 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 мая 2021 г. № 416-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27002:2013 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности» (ISO/IEC 27002:2013 «Information technology — Security techniques — Code of practice for information security controls», IDT), включая технические поправки: Cor.1:2014; Cor.2:2015.

Технические поправки к указанному международному стандарту, принятые после его официальной публикации, внесены в текст настоящего стандарта и выделены двойной вертикальной линией, расположенной на полях соответствующего текста, а обозначение и год принятия технической поправки приведены в скобках после соответствующего текста (в примечании к тексту).

ИСО/МЭК 27002 разработан подкомитетом ПК 27 «Методы и средства обеспечения безопасности ИТ» Совместного технического комитета СТК 1 «Информационные технологии» Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК).

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

5 ВЗАМЕН ГОСТ Р ИСО/МЭК 27002—2012

6 Некоторые положения международного стандарта, указанного в пункте 4, могут являться объектом патентных прав. ИСО и МЭК не несут ответственности за идентификацию подобных патентных прав

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)*

## Содержание

# Введение

## 0.1 Общие положения

Настоящий стандарт предназначен для использования организациями в качестве справочного материала при выборе мер обеспечения информационной безопасности (ИБ) в процессе внедрения системы менеджмента информационной безопасности (СМИБ) на основе ИСО/МЭК 27001 [10] или в качестве руководства для организаций, реализующих общепринятые меры обеспечения ИБ. Настоящий стандарт также предназначен для использования при разработке отраслевых руководств и руководств для конкретных организаций по менеджменту информационной безопасности с учетом характерных для них рисков ИБ[1)]).

Организации всех типов и размеров (включая государственный и частный сектор, коммерческие и некоммерческие организации) собирают, обрабатывают, хранят и передают информацию в различной форме, в том числе электронную, физическую и устную (например, переговоры и презентации).

Ценность информации выходит за рамки написанных слов, цифр и изображений: знания, концепции, идеи и бренды являются примерами нематериальных форм информации. Во взаимосвязанном мире информация и связанные с ней процессы, системы, сети и персонал, участвующий в их эксплуатации, обработке и защите, являются активами, которые, как и другие важные бизнес-активы, представляют ценность для бизнеса организации и, следовательно, заслуживают или нуждаются в защите от различных угроз.

Активы подвержены как преднамеренным, так и случайным угрозам, поскольку связанные с ними процессы, системы, сети и люди имеют присущие им уязвимости. Изменения в бизнес-процессах и системах или другие внешние изменения (такие, как новые законы и нормативные акты) могут создавать новые риски ИБ. Следовательно, учитывая множество способов использования уязвимостей угрозами для нанесения вреда организации, риски ИБ всегда будут присутствовать. Эффективная защита информации снижает эти риски, защищая организацию от угроз и уязвимостей, и тем самым уменьшает влияние рисков на ее активы.

ИБ достигается путем внедрения подходящего набора мер обеспечения ИБ, включая политики, процессы, процедуры, организационные структуры и функции программного и аппаратного обеспечения. Эти меры необходимо установить, внедрить, контролировать, пересматривать и улучшать, где это необходимо, для достижения конкретных целей безопасности и бизнеса организации. СМИБ, как это определено в ИСО/МЭК 27001 [10], дает целостное и скоординированное представление о рисках ИБ организации для целей реализации всеобъемлющего набора мер обеспечения ИБ в рамках общей системы менеджмента.

Многие информационные системы не разрабатывались безопасными в контексте ИСО/МЭК 27001 [10] и настоящего стандарта. Безопасность, которая может быть достигнута с помощью технических средств, ограничена и должна поддерживаться надлежащим управлением и процедурами. Процесс определения мер обеспечения ИБ, которые должны быть внедрены, требует тщательного планирования и внимания к деталям. Эффективная СМИБ нуждается в поддержке со стороны всех работников организации. Также может потребоваться участие акционеров, поставщиков или других внешних сторон. Кроме того, могут потребоваться консультации внешних специалистов.

В более общем смысле внедрение эффективной СМИБ повышает уверенность руководства и других заинтересованных сторон в том, что активы организации находятся в безопасности и защищены от вреда, тем самым способствуя ведению бизнеса.

## 0.2 Требования информационной безопасности

Крайне важно, чтобы организация определила применимые требования безопасности. Существует три основных источника требований безопасности:

a) оценка рисков для организации с учетом общей бизнес-стратегии и целей организации. Посредством оценки риска выявляют угрозы активам, оценивают уязвимости, вероятности возникновения и предполагаемое потенциальное воздействие;

b) юридические, законодательные, нормативные и договорные требования, которые должна выполнять организация, ее торговые партнеры, подрядчики и поставщики услуг, а также их социально-культурная среда;

---

[1)] Положения настоящего стандарта должны рассматриваться с учетом требований национальных нормативных актов и стандартов Российской Федерации в области защиты информации.

c) набор принципов, целей и требований бизнеса по обращению, обработке, хранению, передаче и архивированию информации, которые организация разработала для поддержки своей деятельности.

Ресурсы, используемые для внедрения мер обеспечения ИБ, должны быть соизмеримы с ущербом для бизнеса, к которому могут привести проблемы безопасности при отсутствии этих мер. Результаты оценки рисков могут стать основанием для принятия соответствующих решений руководством и помогут расставить приоритеты для управления рисками ИБ и внедрения мер обеспечения ИБ, выбранных для защиты от этих рисков.

ИСО/МЭК 27005 [11] предоставляет руководство по менеджменту рисков ИБ, которое включает в себя рекомендации по оценке, коммуникации, мониторингу и пересмотру рисков.

### 0.3 Выбор мер обеспечения информационной безопасности

Меры обеспечения ИБ могут быть выбраны как из настоящего стандарта, так и из других источников. При необходимости могут быть разработаны новые меры для удовлетворения специфичных потребностей организации.

Выбор мер обеспечения ИБ зависит от организационных решений, основанных на критериях принятия риска, вариантах обработки риска и общем подходе к управлению рисками, применяемом в организации, а также должен учитывать соответствующее национальное и международное законодательство и нормативное регулирование. При выборе мер для обеспечения надежной информационной безопасности необходимо предполагать, как меры могут взаимодействовать между собой.

Некоторые из мер обеспечения ИБ, приведенных в настоящем стандарте, могут рассматриваться как руководство по менеджменту ИБ и применимы для большинства организаций. Информация о мерах обеспечения ИБ и руководстве по их применению приведена ниже. Более подробная информация о выборе мер обеспечения ИБ и других вариантах обработки риска содержится в ИСО/МЭК 27005 [11].

### 0.4 Разработка собственных рекомендаций

Настоящий стандарт можно рассматривать как основу для разработки рекомендаций, специфичных для организации. Не все меры обеспечения ИБ и рекомендации из настоящего свода норм и правил могут быть применимы. Кроме того, могут потребоваться дополнительные меры и рекомендации, не включенные в настоящий стандарт. В документы, содержащие дополнительные рекомендации или меры, где это применимо, полезно включать перекрестные ссылки на соответствующие пункты настоящего стандарта для облегчения проведения проверки соответствия аудиторами и партнерами по бизнесу.

### 0.5 Вопросы жизненного цикла

Информация имеет свой естественный жизненный цикл, начинающийся от ее создания, проходящий через хранение, обработку, использование и передачу и заканчивающийся ее устареванием или полным уничтожением. Ценность активов и риски для них могут изменяться в течение жизненного цикла (например, ущерб от несанкционированного раскрытия или от кражи финансовых отчетов компании менее значителен после их официального опубликования), однако ИБ в разной степени важна на всех этапах жизненного цикла.

ИБ должна приниматься во внимание на каждом этапе жизненного цикла информационных систем, в пределах которого они планируются, конкретизируются, проектируются, разрабатываются, тестируются, внедряются, используются, поддерживаются и выводятся из эксплуатации. Новые системные разработки и изменения в существующих системах предоставляют организациям возможность обновления и совершенствования мер обеспечения ИБ, принимая во внимание совершившиеся инциденты, а также текущие и прогнозируемые риски ИБ.

### 0.6 Связанные стандарты

В то время как настоящий стандарт содержит руководство по применению достаточно широкого комплекса мер обеспечения ИБ, универсально применимого во множестве организаций различного типа, в других стандартах семейства ИСО/МЭК 27000 представлены дополнительные рекомендации или требования в отношении других частных аспектов менеджмента ИБ.

Для общего ознакомления как с системой менеджмента информационной безопасности, так и с семейством стандартов следует обращаться к ИСО/МЭК 27000. Данный стандарт содержит глоссарий, формально определяющий большинство терминов, используемых в семействе стандартов ИСО/МЭК 27000, и описывает сферу и предназначение других стандартов этого семейства.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Информационные технологии**

# МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

## Свод норм и правил применения мер обеспечения информационной безопасности

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

**Дата введения — 2021—11—30**



## 1 Область применения

В настоящем стандарте содержатся рекомендации по созданию и практическому использованию в организации системы менеджмента информационной безопасности (СМИБ), включая вопросы выбора, внедрения и применения полноценного набора мер обеспечения ИБ, соответствующих совокупности имеющихся в данной организации рисков ИБ.

Настоящий стандарт предназначен для использования организациями, которые намерены:

a) выбрать меры обеспечения ИБ в процессе внедрения системы менеджмента информационной безопасности на основе ИСО/МЭК 27001 [10];

b) внедрить общепринятые меры обеспечения ИБ;

c) разработать свои собственные руководства по менеджменту ИБ.

## 2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт. Для датированных ссылок применяют только указанное издание, для недатированных — последнее издание (включая все изменения).

ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary (Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология)

## 3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 27000.

## 4 Структура стандарта

Настоящий стандарт состоит из 14 разделов, содержащих в совокупности 114 конкретных мер обеспечения ИБ, сгруппированных в 35 основных категорий.

### 4.1 Разделы

Каждый раздел, посвященный мерам обеспечения ИБ, содержит описание одной или нескольких основных категорий.

**Издание официальное**

Порядок следования разделов в настоящем стандарте не отражает их важности. В зависимости от обстоятельств меры обеспечения ИБ из одного или всех разделов могут быть применимы, поэтому каждая организация при использовании настоящего стандарта должна определить важность и применимость мер для себя и отдельных бизнес-процессов. Кроме того, порядок следования пунктов в разделах настоящего стандарта не предполагает распределения их по приоритету.

### 4.2 Категории мер обеспечения информационной безопасности

Каждая основная категория содержит:

a) цель применения мер, которая содержит описание того, что должно быть достигнуто;

b) одну или несколько мер обеспечения ИБ, которые могут быть применены для достижения цели применения меры.

Описание меры обеспечения ИБ структурировано следующим образом:

Мера обеспечения ИБ

Определяет конкретную формулировку меры, направленную на достижение цели применения меры.

Руководство по применению

Предоставляет более подробную информацию для помощи в реализации меры и достижения целей управления. Руководство может не совсем подходить или быть недостаточным для всех ситуаций и может не соответствовать специфичным требованиям организации к мере обеспечения ИБ.

Дополнительная информация

Содержит дополнительную информацию, которую следует принять во внимание, например вопросы юридического характера или ссылки на другие стандарты. Если дополнительной информации нет, то эта часть отсутствует.

## 5 Политики информационной безопасности

### 5.1 Руководящие указания в части информационной безопасности

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

#### 5.1.1 Политики информационной безопасности

Мера обеспечения ИБ

Совокупность политик ИБ должна быть определена, утверждена руководством, опубликована и доведена до сведения всех работников организации и соответствующих внешних сторон.

Руководство по применению

На высоком уровне организация должна определить «политику ИБ», которую утверждает руководство и в которой изложен подход организации к достижению целей ИБ.

Политики ИБ должны учитывать требования, порождаемые:

a) бизнес-стратегией;

b) нормативными актами, требованиями регуляторов, договорами;

c) текущей и прогнозируемой средой угроз ИБ.

Политика ИБ должна содержать положения, касающиеся:

a) определения ИБ, целей и принципов, которыми необходимо руководствоваться в рамках деятельности, связанной с ИБ;

b) определения ролей по менеджменту ИБ и распределения общих и конкретных обязанностей;

c) процессов обработки отклонений и исключений;

d) лиц, несущих ответственность за неисполнение политик ИБ.

На более низком уровне политику ИБ необходимо поддерживать политиками, относящимися к конкретным направлениям в обеспечении ИБ, которые далее предусматривают внедрение мер обеспечения ИБ и, как правило, структурируются для удовлетворения потребностей определенных групп в организации или для охвата определенных областей.

Примерами таких областей политик могут быть:

a) управление доступом (раздел 9);

b) категорирование и обработка информации (см. 8.2);

c) физическая безопасность и защита от воздействия окружающей среды (раздел 11);

d) области, ориентированные на конечного пользователя:
   1) допустимое использование активов (см. 8.1.3);
   2) «чистый стол» и «чистый экран» (см. 11.2.9);
   3) передача информации (см. 13.2.1);
   4) мобильные устройства и дистанционная работа (см. 6.2);
   5) ограничения на установку и использование программного обеспечения (см. 12.6.2);
e) резервное копирование (см. 12.3);
f) передача информации (см.13.2);
g) защита от вредоносных программ (см. 12.2);
h) управление техническими уязвимостями (см. 12.6.1);
i) криптография (раздел 10);
j) безопасность коммуникаций (раздел 13);
k) конфиденциальность и защита персональных данных (см. 18.1.4);
l) взаимоотношения с поставщиками (раздел 15).

Эти политики должны быть доведены до сведения всех работников и причастных внешних сторон в актуальной, доступной и понятной для предполагаемого читателя форме, например в контексте «программы информирования, обучения и практической подготовки (тренинги) в области информационной безопасности» (см. 7.2.2).

Дополнительная информация

Потребность во внутренних политиках ИБ варьируется в зависимости от организации. Внутренние политики особенно полезны в крупных организациях, где лица, определяющие и утверждающие необходимый уровень мер обеспечения ИБ, отделены от лиц, реализующих эти меры; или в ситуациях, когда политика распространяется на многих людей или на многие функции в организации. Политики ИБ могут быть оформлены в виде единого документа, например «Политика информационной безопасности», или в виде набора отдельных, но связанных документов.

Если какие-либо политики ИБ распространяются за пределы организации, то следует следить за тем, чтобы никакая конфиденциальная информация не была разглашена.

Некоторые организации используют другие термины для документов-политик, например «Стандарты», «Инструкции», «Правила».

#### 5.1.2 Пересмотр политик информационной безопасности

Мера обеспечения ИБ

Политики ИБ должны пересматриваться через запланированные интервалы времени или в случае происходящих существенных изменений для обеспечения уверенности в сохранении их приемлемости, адекватности и результативности.

Руководство по применению

Каждой политике должен быть назначен владелец, за которым утверждена ответственность по разработке, пересмотру и оценке. Пересмотр должен включать в себя оценку возможностей для улучшения политик организации и подхода к менеджменту ИБ в ответ на изменения в среде организации, обстоятельств бизнеса, применимых нормативных и правовых актах или технической среде.

При пересмотре политик ИБ следует учитывать результаты проверок со стороны высшего руководства.

Высшее руководство должно утвердить пересмотренную политику.

## 6 Организация деятельности по информационной безопасности

### 6.1 Внутренняя организация деятельности по обеспечению информационной безопасности

Цель: Создать структуру органов управления для инициирования и контроля внедрения и функционирования ИБ в организации.

#### 6.1.1 Роли и обязанности по обеспечению информационной безопасности

Мера обеспечения ИБ

Все обязанности по обеспечению ИБ должны быть определены и распределены.

Руководство по применению

Разделение обязанностей по обеспечению ИБ необходимо осуществлять в соответствии с политиками ИБ (см. 5.1.1). Должны быть определены обязанности по защите конкретных активов и выполнению конкретных процессов ИБ. Там, где это необходимо, обязанности следует дополнять более подробным руководством для конкретных мест и средств обработки информации.

Лица, за которыми закреплены обязанности, связанные с ИБ, могут делегировать задачи по обеспечению безопасности другим. Но поскольку ответственность остается лежать на них, они должны удостовериться, что все делегированные задачи были выполнены корректно.

Должны быть определены области, за которые лица несут ответственность. В частности, следует проделать следующее:

a) активы и процессы ИБ должны быть идентифицированы и описаны;

b) для каждого актива или процесса ИБ следует назначить ответственное лицо, при этом следует детально задокументировать возложенную ответственность;

c) должны быть определены и задокументированы уровни полномочий;

d) чтобы иметь возможность выполнять возложенные обязанности, назначенные лица должны быть компетентны в области ИБ и им должна быть предоставлена возможность поддержания своих компетенций на должном уровне;

e) должны быть определены и задокументированы аспекты взаимодействия и контроля ИБ при взаимодействии с поставщиками.

Дополнительная информация

Многие организации назначают менеджера по ИБ, который в целом несет ответственность за разработку и внедрение системы менеджмента информационной безопасности и за выбор мер обеспечения ИБ.

Тем не менее, ответственность за выделение ресурсов и внедрение мер обеспечения ИБ часто ложится на отдельных менеджеров. Распространенной практикой является назначение владельца каждому активу, который затем становится ответственным за его постоянную защиту.

**6.1.2 Разделение обязанностей**

Мера обеспечения ИБ

Пересекающиеся обязанности и зоны ответственности должны быть разделены для уменьшения возможности несанкционированного или непреднамеренного изменения или нецелевого использования активов организации.

Руководство по применению

Следует позаботиться о том, чтобы одно и то же лицо не могло получить доступ к активам, изменять или использовать их без разрешения или возможности обнаружения такого действия. Инициирование события должно быть отделено от его авторизации. При разработке мер обеспечения ИБ следует учитывать возможность сговора.

Небольшие организации могут столкнуться с трудностями при разделении обязанностей, тем не менее данный принцип следует применять настолько, насколько это возможно и практически осуществимо. Там, где возникают трудности с разделением обязанностей, следует рассмотреть другие меры обеспечения ИБ, такие как мониторинг деятельности, ведение записей в журналах и контроль со стороны руководства.

Дополнительная информация

Разделение обязанностей — это метод снижения риска случайного или преднамеренного ненадлежащего использования активов организации.

**6.1.3 Взаимодействие с органами власти**

Мера обеспечения ИБ

Должны поддерживаться соответствующие контакты с уполномоченными органами власти.

Руководство по применению

В организациях должны действовать процедуры, определяющие, в каких случаях и кому следует связываться с органами власти (например, с правоохранительными, регулирующими или надзорными органами), и каким образом информация о выявленных инцидентах ИБ должна своевременно передаваться (например, если есть подозрения на возможное нарушение закона).

Дополнительная информация

Организации, подвергающиеся атакам из сети Интернет, вероятнее всего будут нуждаться в обращении к органам власти для принятия мер обеспечения ИБ против источника атаки.

Поддержание таких контактов может являться требованием, обеспечивающим менеджмент инцидентов ИБ (раздел 16) или процесс непрерывности бизнеса и действий в чрезвычайных ситуациях (раздел 17). Взаимодействие с регулирующими органами также полезно для прогнозирования и подготовки к предстоящим изменениям в законах и нормативных актах, применимых к организации. Стоит поддерживать контакты и с другими органами, такими как коммунальные и аварийные службы, поставщики электроэнергии, службы спасения, например пожарные (в связи с обеспечением непрерывности бизнеса), провайдеры телекоммуникационных услуг (в связи с обеспечением доступности линий связи и маршрутизацией), службы водоснабжения (для обеспечения своевременного охлаждения оборудования).

**6.1.4 Взаимодействие с профессиональными сообществами**

Мера обеспечения ИБ

Должно поддерживаться соответствующее взаимодействие с заинтересованными профессиональными сообществами и ассоциациями или форумами, проводимыми специалистами по безопасности.

Руководство по применению

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

a) получения актуальной информации о происходящем в сфере ИБ и расширения знаний о лучших практиках;

b) обеспечения актуальности и полноты понимания среды ИБ;

c) получения заблаговременных оповещений об опасностях, рекомендациях и исправлениях, касающихся атак и уязвимостей;

d) получения консультаций у специалистов по ИБ;

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

f) обеспечения подходящих точек взаимодействия при обработке инцидентов ИБ (раздел 16).

Дополнительная информация

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

**6.1.5 Информационная безопасность при управлении проектом**

Мера обеспечения ИБ

ИБ должна рассматриваться при управлении проектом независимо от типа проекта.

Руководство по применению

ИБ должна быть интегрирована в метод(ы) управления проектами, чтобы гарантировать, что риски ИБ идентифицированы и обработаны в рамках проекта. Обычно это относится к любому проекту независимо от его характера, например проект для основного бизнес-процесса, ИТ, управления объектами и других вспомогательных процессов. Применяемые методы управления проектами должны предусматривать, что:

a) цели ИБ включены в цели проекта;

b) оценку риска ИБ проводят на ранней стадии проекта для определения необходимых вариантов его обработки;

c) ИБ является частью всех этапов применяемой методологии проекта.

Последствия для ИБ следует регулярно анализировать и пересматривать во всех проектах. Ответственность за ИБ должна быть установлена и распределена между точно определенными ролями, которые заданы в методах управления проектом.

### 6.2 Мобильные устройства и дистанционная работа

| |
|---|
| Цель: Обеспечить безопасность при дистанционной работе и использовании мобильных устройств. |

**6.2.1 Политика использования мобильных устройств**

Мера обеспечения ИБ

Должна быть определена политика и реализованы поддерживающие меры обеспечения ИБ для управления рисками ИБ, связанными с использованием мобильных устройств.

Руководство по применению

При использовании мобильных устройств особое внимание следует уделять тому, чтобы информация ограниченного доступа не была скомпрометирована. Политика использования мобильных устройств должна принимать во внимание риски работы с мобильными устройствами в незащищенных средах.

Политика использования мобильных устройств должна предусматривать:

a) регистрацию мобильных устройств;

b) требования к физической защите;

c) ограничения на установку программного обеспечения;

d) требования к версиям программного обеспечения мобильного устройства и применению исправлений;

e) ограничение подключения к информационным сервисам;

f) управление доступом;

g) криптографические методы обеспечения ИБ;

h) защиту от вредоносного программного обеспечения;

i) возможности дистанционного отключения, стирания или блокировки;

j) резервное копирование;

k) использование веб-сервисов и веб-приложений;

l) контроль получения прав «root» на устройстве.

Следует проявлять осторожность при использовании устройств в общественных местах, конференц-залах и других незащищенных местах. Должна быть предусмотрена защита от несанкционированного доступа или раскрытия информации, хранящейся и обрабатываемой этими устройствами, например, использование криптографических методов (раздел 10) и принудительное применение секретной аутентификационной информации (см. 9.2.4).

Мобильные устройства также должны быть физически защищены от кражи, особенно если они могут быть оставлены, например, в автомобилях и других видах транспорта, в гостиничных номерах, конференц-центрах и местах для встреч. Для случаев кражи или утери мобильных устройств должна быть установлена специальная процедура, учитывающая правовые, страховые и другие требования безопасности организации. Устройства, несущие важную, ограниченную информацию, не следует оставлять без присмотра и, по возможности, их следует физически запирать или использовать специальные замки для защиты.

Следует организовать обучение персонала, использующего мобильные устройства, для повышения их осведомленности о дополнительных рисках, связанных с таким способом работы, и о мерах обеспечения ИБ, которые должны быть выполнены.

Там, где политика допускает использование личных мобильных устройств, политика и соответствующие меры обеспечения ИБ также должны предусматривать:

a) разделение использования устройств в личных и рабочих целях, включая использование программного обеспечения для обеспечения такого разделения и защиты информации ограниченного доступа на личном устройстве;

b) предоставление доступа к информации ограниченного доступа только после того, как пользователи подпишут соглашение, признающее их обязанности (физическая защита, обновление программного обеспечения и т. д.), отказ от владения информацией ограниченного доступа, позволяющее организации дистанционно удалять данные в случае кражи или утери устройства, или когда пользователь больше не авторизован на использование. Политика должна учитывать особенности законодательства по защите конфиденциальной информации.

Дополнительная информация

Беспроводные сети для мобильных устройств похожи на другие типы сетей, однако имеют важные отличия, которые необходимо учитывать при определении мер обеспечения ИБ. Типичными отличиями являются:

a) некоторые беспроводные протоколы, обеспечивающие безопасность, недостаточно развиты и имеют известные недостатки;

b) информация, хранящаяся на мобильных устройствах, может быть не скопирована из-за ограниченной пропускной способности сети или из-за того, что мобильные устройства могут оказаться не подключены к сети во время запланированного резервного копирования.

Мобильные устройства обычно имеют общие функции со стационарно используемыми устройствами, например доступ в сеть и Интернет, электронная почта и управление файлами. Меры обеспече-

ния ИБ для мобильных устройств, как правило, состоят из адаптированных мер, которые используются в стационарных устройствах и тех, которые предназначены для устранения угроз, возникающих при их использовании вне помещений организации.

**6.2.2 Дистанционная работа**

Мера обеспечения ИБ

Должна быть определена политика и реализованы поддерживающие меры безопасности для защиты информации, доступ к которой, обработку или хранение осуществляют в местах дистанционной работы.

Руководство по применению

В организациях, предусматривающих возможность дистанционной работы, должна издаваться политика, определяющая условия и ограничения для дистанционной работы. В тех случаях, когда это применимо и разрешено законом, следует рассмотреть следующие вопросы:

a) существующая физическая защита удаленного места работы с учетом физической безопасности здания и местности;

b) предлагаемая физическая среда дистанционной работы;

c) требования к безопасности связи с учетом необходимости удаленного доступа к внутренним системам организации, чувствительности этих систем, а также с учетом информации ограниченного доступа, к которой будут осуществлять доступ и которую будут передавать по линиям связи;

d) предоставление доступа к виртуальному рабочему столу, который предотвращает обработку и хранение информации на личном оборудовании;

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

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

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

h) доступ к личному оборудованию (для проверки его безопасности или в ходе расследования) может быть запрещен законодательством;

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

j) требования к защите от вредоносных программ и межсетевым экранам.

Руководящие принципы и меры, которые следует учитывать, должны включать в себя:

a) предоставление подходящего оборудования для дистанционной работы и устройств хранения в тех случаях, когда использование личного оборудования, не находящегося под контролем организации, не допускается;

b) определение разрешенных работ, часов работы, категорий информации, которую можно обрабатывать, а также определение внутренних систем и сервисов, к которым разрешен доступ дистанционному работнику;

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

d) физическую безопасность;

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

f) предоставление технической и программной поддержки и обслуживания;

g) страхование;

h) процедуры резервного копирования и обеспечения непрерывности бизнеса;

i) аудит и мониторинг безопасности;

j) аннулирование полномочий и прав доступа, а также возврат оборудования по окончании дистанционной работы;

k) предоставление доступа к корпоративной информации.

Дополнительная информация

К термину «дистанционная работа» относятся все формы работы вне офиса, в том числе нетрадиционная рабочая среда, такая как «работа на дому», «гибкое рабочее место» и «виртуальное рабочее место».

# 7 Безопасность, связанная с персоналом

## 7.1 При приеме на работу

Цель: Обеспечить уверенность в том, что работники и подрядчики понимают свои обязанности и подходят для роли, на которую они рассматриваются.

### 7.1.1 Проверка

Мера обеспечения ИБ

Проверка всех кандидатов при приеме на работу должна осуществляться согласно соответствующим законам, правилам и этическим нормам и должна быть соразмерна требованиям бизнеса, категории информации, которая будет доступна, и предполагаемым рискам ИБ.

Руководство по применению

Проверку следует проводить принимая во внимание обеспечение конфиденциальности, защиту персональных данных и законодательство о трудоустройстве, и там, где это разрешено, она должна включать в себя следующее:

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

b) проверку (на полноту и точность) биографии заявителя;

c) подтверждение заявленного образования и профессиональной квалификации;

d) независимую проверку личности (паспорт или иной подобный документ);

e) более детальную проверку, такую как обзор кредитной истории или проверку судимостей.

Когда работника принимают на работу для выполнения определенной роли ИБ, необходимо удостовериться, что кандидат:

a) обладает необходимыми компетенциями для этой роли;

b) имеет высокий уровень доверия, особенно если роль имеет важное значение для организации.

В случаях, когда работнику после приема на работу или при продвижении по службе предоставляется обязательный доступ к конфиденциальной информации, и, в частности, обрабатывающим конфиденциальную информацию, например финансовую или секретную, организации следует проводить дальнейшие, более детальные, проверки.

Процедуры должны определять критерии и ограничения для процесса перепроверки работников, например, кто, как, когда и с какой целью проводит эту перепроверку.

Процесс проверки также следует обеспечивать в отношении подрядчиков. В этих случаях в соглашении между сторонами должны быть четко указаны обязанности по проведению проверки и процедуры уведомлений, которые необходимо соблюдать, если проверка не была завершена или если результаты дают основания для сомнений или опасений.

Информацию обо всех рассматриваемых кандидатах, претендующих на занятие должностей в организации, следует собирать и обрабатывать согласно действующему в соответствующей юрисдикции законодательству. В зависимости от применимого законодательства может понадобиться предварительное информирование кандидата о проверке.

### 7.1.2 Правила и условия работы

Мера обеспечения ИБ

В договорных соглашениях с работниками и подрядчиками должны быть установлены их обязанности и обязанности организации по обеспечению ИБ.

Руководство по применению

Договорные обязательства для работников и подрядчиков должны отражать политики организации в области ИБ, дополнительно уточняя и утверждая:

a) что все работники и подрядчики, которым предоставляется доступ к конфиденциальной информации, должны подписать соглашение о конфиденциальности или неразглашении до получения доступа к средствам обработки информации (см. 13.2.4);

b) юридическую ответственность и права работника или подрядчика, например в отношении законов об авторском праве или защите данных (см. 18.1.2 и 18.1.4);

c) обязанности по категорированию информации и управлению информацией организации, иными активами, связанными с информацией, средствами ее обработки и информационными системами, используемыми работником или подрядчиком (раздел 8). (Внесена техническая поправка Cor.1:2014);

d) ответственность работника или подрядчика за обработку информации, полученной от других компаний или внешних сторон;

e) действия, которые необходимо предпринять, если работник или подрядчик не соблюдает требования безопасности организации (см. 7.2.3).

Роли и обязанности в области ИБ должны быть доведены до сведения кандидатов до их приема на работу.

Организация должна обеспечивать уверенность в том, что работники и подрядчики согласны с условиями, касающимися ИБ, соответствующими характеру и уровню доступа, который они будут иметь к активам организации, связанным с информационными системами и сервисами.

Там, где это применимо, действие обязанностей, содержащихся в правилах и условиях работы, должно быть продлено на определенный период после прекращения трудовых или договорных отношений (см. 7.3).

Дополнительная информация

Для установления обязанностей работника или подрядчика в отношении конфиденциальности, защиты данных, этики, приемлемого использования активов и средств организации, а также ожидаемого организацией следования признанным практикам может быть использован кодекс поведения. Внешняя сторона, с которой связан подрядчик, может быть обязана вступить в договорные соглашения от имени подрядчика, подписавшего договор.

### 7.2 Во время работы

Цель: Обеспечить уверенность в том, что работники и подрядчики осведомлены о своих обязанностях в отношении ИБ и выполняют их.

#### 7.2.1 Обязанности руководства организации

Мера обеспечения ИБ

Руководство организации должно требовать от всех работников и подрядчиков соблюдения ИБ в соответствии с установленными в организации политиками и процедурами.

Руководство по применению

В обязанности руководства входит обеспечение того, чтобы работники и подрядчики:

a) были надлежащим образом проинформированы об их ролях и обязанностях в области ИБ до предоставления доступа к конфиденциальной информации или информационным системам;

b) были обеспечены рекомендациями, которые устанавливают ожидания по ИБ для их роли в организации;

c) были мотивированы выполнять политики ИБ организации;

d) были осведомлены об ИБ настолько, насколько это предполагают их роли и обязанности в организации (см. 7.2.2);

e) соблюдали правила и условия работы, в том числе политику ИБ организации и соответствующие методы работы;

f) поддерживали соответствующий уровень навыков и квалификацию, а также регулярно проходили обучение;

g) имели канал для анонимного сообщения о нарушениях политик или процедур ИБ («информирование о нарушениях»).

Руководство должно демонстрировать поддержку политик, процедур и мер обеспечения ИБ и выступать в качестве образца для подражания.

Дополнительная информация

Если работники и подрядчики не осведомлены о своих обязанностях в области ИБ, то они могут нанести значительный ущерб организации. Гораздо надежнее иметь мотивированный персонал, который, вероятно, будет вызывать меньше инцидентов ИБ.

Недостаточное управление может привести к тому, что персонал будет чувствовать себя недооцененным, что может привести к негативному влиянию на ИБ в организации. Например, плохое управление может привести к игнорированию требований ИБ или возможному неприемлемому использованию активов организации.

**7.2.2 Осведомленность, обучение и практическая подготовка (тренинги) в области информационной безопасности**

Мера обеспечения ИБ

Все работники организации и при необходимости подрядчики должны быть надлежащим образом обучены, практически подготовлены и на регулярной основе осведомлены об обновлениях политик и процедур ИБ организации, необходимых для выполнения их функциональных обязанностей.

Руководство по применению

Программа повышения осведомленности в области ИБ должна быть направлена на то, чтобы работники и, в соответствующих случаях, подрядчики понимали свои обязанности по обеспечению ИБ и средства, с помощью которых эти обязанности следует выполнять.

Программа повышения осведомленности в области ИБ должна быть разработана в соответствии с политикой и соответствующими процедурами ИБ организации, принимая во внимание информацию и меры обеспечения ИБ, которые внедрены для ее защиты. Программа должна включать в себя ряд мероприятий, таких как кампании по повышению осведомленности (например, «День информационной безопасности») и выпуск буклетов или информационных бюллетеней.

Программу повышения осведомленности необходимо планировать с учетом роли работников в организации и, при необходимости, ожиданий организации в отношении осведомленности подрядчиков. Мероприятия в рамках программы должны быть рассчитаны на длительный период, предпочтительно быть регулярными, повторяться и охватывать новых работников и подрядчиков. Следует регулярно обновлять программу, чтобы она соответствовала политикам и процедурам организации и основывалась на уроках, извлеченных из инцидентов ИБ.

Практическая реализация программы повышения осведомленности должна проводиться в соответствии с требованиями программы. В качестве методов можно использовать обучение в классе, дистанционное обучение, сетевое обучение, самостоятельное изучение и другие методы.

Обучение и практическая подготовка в области ИБ должна также охватывать общие аспекты, такие как:

a) заявление руководства о приверженности ИБ во всей организации;

b) необходимость ознакомления с правилами и обязательствами, применяемыми в области ИБ, определенными в политиках, стандартах, законах, положениях, договорах и соглашениях;

c) персональная ответственность за свои действия и бездействие, а также общая ответственность за обеспечение безопасности или защиту информации, принадлежащей организации и внешним сторонам;

d) базовые процедуры ИБ (такие как сообщение об инцидентах ИБ) и базовые меры обеспечения ИБ (такие как парольная защита, защита от вредоносного программного обеспечения или «чистый стол»);

e) контакты и ресурсы для получения дополнительной информации и консультаций по вопросам ИБ, включая дополнительные материалы по обучению и подготовке в области ИБ.

Обучение и практическую подготовку по ИБ следует проводить на периодичной основе. Вводный курс следует проходить не только новым работникам, но и тем, кто переводится на новую должность или получает роль с существенно отличающимися требованиями ИБ, при этом обучение следует проводить заранее.

Для большей результативности организация должна разработать программу обучения и практической подготовки. Программа должна соответствовать политике ИБ организации и соответствующим процедурам, принимая во внимание защищаемую информацию и меры, которые были внедрены для обеспечения ее защиты. Программа должна учитывать возможность реализации различных форм обучения и подготовки, например лекции или самостоятельные занятия.

Дополнительная информация

Программа повышения осведомленности в области ИБ должна основываться на различном уровне ценности информационных активов, а также на мировой практике негативных событий в области ИБ.

Процесс повышения осведомленности должен быть соотнесен с имеющейся загрузкой работников организации и, по возможности, должен занимать у работников максимально короткое время, при этом обучая их самым значимым аспектам ИБ.

При формировании программы повышения осведомленности важно сфокусироваться не только на «что» и «как», но и на «почему». Важно, чтобы работники понимали цель ИБ и потенциальное влияние, положительное или отрицательное, их действий на организацию.

Осведомленность, обучение и практическая подготовка могут быть частью или проводиться совместно с другими обучающими мероприятиями, например общими тренингами в области информационных технологий или безопасности. Мероприятия по повышению осведомленности, обучению и практической подготовке должны соответствовать конкретным ролям, обязанностям и навыкам.

В конце курса по повышению осведомленности, обучению и практической подготовке может быть проведена оценка знаний по пройденным материалам.

**7.2.3 Дисциплинарный процесс**

Мера обеспечения ИБ

Должен существовать формализованный и доведенный до персонала дисциплинарный процесс по принятию мер в отношении работников, совершивших нарушение ИБ.

Руководство по применению

Дисциплинарный процесс не должен быть инициирован, пока не будет уверенности в том, что нарушение ИБ действительно имело место (см. 16.1.7).

Формальный дисциплинарный процесс должен обеспечивать корректное и справедливое обращение с работниками, которые подозреваются в совершении нарушений ИБ. Формальный дисциплинарный процесс должен предусматриваться как соответствующий ответ, учитывающий такие факторы, как характер и серьезность нарушения и его влияние на бизнес, первое это нарушение или повторное, проходил ли нарушитель надлежащее обучение, соответствующее законодательство, бизнес-контракты и другие необходимые факторы.

Дисциплинарный процесс также должен использоваться в качестве сдерживающего фактора для предотвращения нарушения работниками как политик и процедур ИБ, так и иных нарушений в этой области. Умышленные нарушения должны требовать немедленного реагирования.

Работник обязан соблюдать политику информационной безопасности. При несоблюдении политики информационной безопасности работодатель вправе обратиться в правоохранительные органы для привлечения к ответственности своего рабочего.

Дополнительная информация

Дисциплинарный процесс также может стать мотивацией или стимулом, если будут определены меры поощрения в случае образцового выполнения требований ИБ.

**7.3 Увольнение и смена места работы**

| |
|---|
| Цель: Защита интересов организации при смене места работы или увольнении работника. |

**7.3.1 Прекращение или изменение трудовых обязанностей**

Мера обеспечения ИБ

Ответственность и обязанности, относящиеся к ИБ, которые сохраняются после увольнения или смены места работы, должны быть определены, доведены до сведения работника или подрядчика и оформлены юридически.

Руководство по применению

Сообщение об увольнении должно включать в себя текущие требования ИБ и юридические обязательства и, где это применимо, обязательства, содержащиеся в соглашениях о конфиденциальности (см. 13.2.4), а также в правилах и условиях работы (см. 7.1.2), сохраняющие свою силу в течение определенного периода времени после окончания работы работника или подрядчика.

Ответственность и обязанности, которые остаются в силе после увольнения, должны быть закреплены в правилах и условиях работы работника или подрядчика (см. 7.1.2). Изменение должностных обязанностей или функций следует проводить так же, как и в случае с увольнением, при этом дополнив возложением новых должностных обязанностей и функций.

Дополнительная информация

Отдел по управлению персоналом, как правило, отвечает за общий процесс увольнения и взаимодействует с руководителем увольняемого лица касательно выполнения соответствующих процедур, относящихся к ИБ. В отношении подрядчика данный процесс осуществляется внешней стороной в соответствии с заключенным с ней договором.

Работников и подрядчиков необходимо информировать об изменениях в штате и порядке работы.

# 8 Менеджмент активов

## 8.1 Ответственность за активы

Цель: Идентификация активов организации и определение соответствующих обязанностей по их защите.

### 8.1.1 Инвентаризация активов

Мера обеспечения ИБ

Информация, средства обработки информации и другие активы, связанные с информацией, должны быть идентифицированы, а также должен быть составлен и поддерживаться в актуальном состоянии перечень этих активов. (Внесена техническая поправка Cor.1:2014).

Руководство по применению

Организация должна идентифицировать активы, относящиеся к жизненному циклу информации, и задокументировать их значимость. Жизненный цикл информации должен включать в себя создание, обработку, хранение, передачу, удаление и уничтожение. Документация должна храниться в специально созданных или уже существующих перечнях, в зависимости от ситуации.

Перечень активов должен быть точным, актуальным, полным и согласованным с другими инвентаризационными перечнями.

Для каждого актива, включенного в перечень, должен быть определен его владелец (см. 8.1.2) и проведено категорирование (см. 8.2).

Дополнительная информация

Инвентаризация активов помогает обеспечить эффективную защиту и может также потребоваться для других целей, таких как здоровье и безопасность, страхование или финансы (управление активами).

ИСО/МЭК 27005 [11] предоставляет примеры активов, которые могут быть приняты во внимание организацией в процессе идентификации активов. Процесс составления перечня активов является важной предпосылкой управления рисками (см. также ИСО/МЭК 27001 [10] и ИСО/МЭК 27005 [11]).

### 8.1.2 Владение активами

Мера обеспечения ИБ

Для каждого актива, включенного в перечень инвентаризации, должен быть определен его владелец.

Руководство по применению

Отдельные физические лица, так же как и юридические лица, имеющие утвержденную руководством ответственность за актив в течение его жизненного цикла, могут быть назначены в качестве владельцев активов. Владелец актива несет ответственность за выполнение требований ИБ для данного актива.

Как правило, осуществляется процесс, обеспечивающий своевременное назначение владельца актива. Владелец должен быть назначен при создании активов или при передаче активов в организацию. Владелец актива должен нести ответственность за надлежащее управление активом в течение всего жизненного цикла актива.

Владелец актива должен:

a) обеспечить проведение инвентаризации активов;

b) обеспечить, чтобы активы были должным образом категорированы и защищены;

c) определять и периодически пересматривать ограничения доступа и категорирование важных активов с учетом действующих политик управления доступом;

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

Дополнительная информация

Назначенный владелец не обязательно имеет какие-либо права собственности на актив.

Рутинные задачи могут быть делегированы, например ответственному за хранение, который следит за активами ежедневно, но ответственность при этом остается на владельце.

В сложных информационных системах может быть полезно определять группы активов, совместно обеспечивающих определенный сервис. В этом случае владелец этого сервиса является ответственным за его предоставление, включая действия с активами.

**8.1.3 Допустимое использование активов**

Мера обеспечения ИБ

Должны быть идентифицированы, документально оформлены и реализованы правила допустимого использования активов, включая информацию и средства ее обработки.

Руководство по применению

Работники и внешние пользователи, использующие или имеющие доступ к активам организации, должны быть осведомлены о требованиях ИБ, относящихся к информации, активам организации, связанным с информацией, средствам и ресурсам обработки информации. (Внесена техническая поправка Cor.1:2014).

Они должны нести ответственность за использование ими любых ресурсов обработки информации и любое подобное использование, осуществляемое в зоне их ответственности.

**8.1.4 Возврат активов**

Мера обеспечения ИБ

Все работники и внешние пользователи должны возвратить все активы организации, находящиеся в их пользовании, после увольнения, истечения срока действия договора или соглашения.

Руководство по применению

Процесс прекращения трудовых отношений должен быть оформлен таким образом, чтобы включать возврат всех ранее выданных физических и электронных активов, принадлежащих или доверенных организации.

В тех случаях, когда работник или внешний пользователь купил оборудование организации или использует свое личное оборудование, необходимо соблюдать процедуры, обеспечивающие передачу всей соответствующей информации в организацию и ее безопасное удаление из оборудования (см. 11.2.7).

В тех случаях, когда работник или внешний пользователь обладает знаниями, важными для текущей деятельности, такого рода информация должна быть задокументирована и передана в организацию.

В течение некоторого периода времени после уведомления о прекращении трудовых отношений организация должна контролировать неавторизованное копирование соответствующей информации (например, интеллектуальной собственности) увольняемыми работниками и подрядчиками.

**8.2 Категорирование информации**

Цель: Обеспечить уверенность в том, что в отношении информации обеспечивается надлежащий уровень защиты в соответствии с ее значимостью для организации.

**8.2.1 Категорирование информации**

Мера обеспечения ИБ

Информация должна быть категорирована с точки зрения нормативных правовых требований, ценности, критичности и чувствительности к неавторизованному раскрытию или модификации.

Руководство по применению

Категорирование информации и связанные с ней меры обеспечения информационной безопасности должны учитывать потребности бизнеса в обмене информацией или ограничении доступа к ней, а также требования законодательства. Прочие активы, не являющиеся информацией, также могут быть категорированы в соответствии с категорированием информации, которая в них хранится, обрабатывается или иным образом преобразуется, или защищается этими активами.

Владельцы информационных активов должны быть ответственными за их категорирование.

Система категорирования должна включать в себя метки категорирования и критерии для пересмотра категорирования по истечении времени. Уровень защиты в системе должен оцениваться путем анализа конфиденциальности, целостности и доступности и любых других требований к рассматриваемой информации. Система должна быть согласована с политикой управления доступом (см. 9.1.1).

Каждому уровню должно быть присвоено наименование, которое имеет смысл в контексте применения этой системы категорирования.

Система должна быть единой для всей организации, чтобы лица, проводящие категорирование информации и связанных с ней активов, выполняли это одинаково, имели общее понимание требований по защите и применяли соответствующие меры по защите.

Категорирование должно быть включено в процессы организации, быть согласованным и единообразным по всей организации. Результаты категорирования должны отражать ценность активов в зависимости от их чувствительности и критичности для организации, например с точки зрения конфиденциальности, целостности и доступности. Результаты категорирования информации должны обновляться в соответствии с изменениями их ценности, чувствительности и критичности в течение всего их жизненного цикла.

Дополнительная информация

Категорирование предоставляет людям, имеющим дело с информацией, краткое указание о том, как обрабатывать информацию и защищать ее. Создание категорий информации с одинаковыми необходимыми мерами по защите и определение процедур ИБ, которые применяются ко всей информации в каждой категории, облегчает эту задачу. Такой подход снижает потребность в оценке рисков и разработке мер обеспечения информационной безопасности в каждом отдельном случае.

Информация может перестать быть чувствительной или критической по истечении некоторого периода времени, например когда она становится общедоступной. Эти аспекты необходимо принимать во внимание, поскольку присвоение более высокой категории может привести к реализации излишних мер обеспечения ИБ и, как следствие, к дополнительным расходам или, наоборот, присвоение более низкой категории может поставить под угрозу достижение бизнес-целей.

Пример системы категорирования по конфиденциальности информации может основываться на следующих четырех уровнях:

a) раскрытие информации не приведет к ущербу;

b) раскрытие информации приведет к незначительным затруднениям или незначительным неудобствам в операционной деятельности;

c) раскрытие информации оказывает значительное кратковременное влияние на операционную деятельность или достижение тактических целей;

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

**8.2.2 Маркировка информации**

Мера обеспечения ИБ

Должен быть разработан и реализован соответствующий набор процедур маркировки информации в соответствии с принятой в организации системой категорирования информации.

Руководство по применению

Необходимо, чтобы процедуры маркировки информации охватывали информационные активы, представленные как в физической, так и в электронной форме. Маркировка должна соответствовать системе категорирования, установленной в 8.2.1. Маркировка должна легко распознаваться. Процедуры должны содержать указания относительно того, где и как размещается маркировка, с учетом того, каким образом осуществляется доступ к информации или каким образом обрабатываются активы, в зависимости от типов носителей. Процедуры могут определять случаи, когда маркировкой можно пренебречь, например для снижения рабочей загруженности можно пренебречь маркировкой неконфиденциальной информации. Работники и подрядчики должны быть ознакомлены с процедурами маркировки информации.

Результаты, формируемые системами, содержащими информацию ограниченного доступа, должны иметь соответствующую маркировку по категориям.

Дополнительная информация

Маркировка конфиденциальной информации является ключевым требованием для мероприятий по обмену информацией. Физические метки и метаданные являются наиболее распространенными формами меток.

Маркировка информации и связанных с ней активов иногда может иметь негативные последствия. Конфиденциальные активы легче идентифицировать и соответственно украсть внутреннему или внешнему злоумышленнику.

**8.2.3 Обращение с активами**

Мера обеспечения ИБ

Должны быть разработаны и реализованы процедуры обращения с активами в соответствии с принятой в организации системой категорирования информации.

Руководство по применению

Должны быть разработаны процедуры для обращения, обработки, хранения и передачи информации в соответствии с ее категорированием (см. 8.2.1).

Должны быть рассмотрены следующие вопросы:

a) ограничение доступа, обеспечивающее выполнение требований по защите для каждой категории;

b) ведение официального учета уполномоченных обладателей активов;

c) защита временных или постоянных копий информации на уровне, соответствующем уровню защиты оригиналов информации;

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

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

Система категорирования, используемая в организации, может не быть равнозначной схемам, используемым другими организациями, даже если схожи наименования категорий; кроме того, информация, передаваемая между организациями, может относиться к разным категориям в зависимости от ситуации в каждой организации, даже если их системы категорирования идентичны.

Соглашения с другими организациями, предусматривающие обмен информацией, должны включать в себя описание процедур категорирования этой информации и интерпретации категорий информации этих организаций.

### 8.3 Обращение с носителями информации

Цель: Предотвратить несанкционированное раскрытие, модификацию, удаление или уничтожение информации, хранящейся на носителях информации.

#### 8.3.1 Управление съемными носителями информации

Мера обеспечения ИБ

Должны быть реализованы процедуры по управлению сменными носителями информации в соответствии с принятой в организации системой категорирования информации.

Руководство по применению

Необходимо рассмотреть следующие рекомендации в отношении управления съемными носителями.

Для управления съемными носителями должны быть учтены следующие рекомендации:

a) содержимое, в котором отпала необходимость, на любых перезаписываемых носителях, которые могут быть вынесены из организации, должно быть удалено без возможности восстановления;

b) где это необходимо и целесообразно, должно требоваться разрешение на вынос носителей информации из организации, а записи о выносе следует хранить как контрольную запись для аудита;

c) все носители следует хранить в безопасном, надежном месте в соответствии с инструкциями производителей;

d) если конфиденциальность или целостность данных являются важными факторами, следует использовать криптографические методы для защиты данных на съемных носителях;

e) для снижения риска деградации носителей, когда сохраняемые данные все еще необходимы, данные должны быть перенесены на новые носители, прежде чем прежние станут нечитаемыми;

f) несколько копий ценных данных следует хранить на отдельных носителях для снижения риска случайного повреждения или потери данных;

g) для уменьшения возможности потери данных должна быть предусмотрена регистрация съемных носителей информации;

h) съемные диски разрешается использовать только в случаях, обусловленных потребностями бизнеса;

i) в случае необходимости использования съемных носителей перенос информации на них необходимо контролировать.

Все процедуры и уровни авторизации должны быть задокументированы.

#### 8.3.2 Утилизация носителей информации

Мера обеспечения ИБ

При выводе из эксплуатации носителей информации требуется их надежно и безопасно утилизировать, используя формализованные процедуры.

Руководство по применению

Должны быть установлены формализованные процедуры для надежной утилизации носителей для уменьшения риска утечки конфиденциальной информации неавторизованным лицам. Процедуры надежной утилизации носителей, содержащих конфиденциальную информацию, должны соответст-

вовать степени доступности к ограниченной информации. Необходимо рассмотреть следующие вопросы:

a) носители, содержащие конфиденциальную информацию, следует хранить и надежно утилизировать, например посредством сжигания или измельчения, или же стирания информации, если носители планируют использовать для другого приложения в пределах организации;

b) должны существовать процедуры по выявлению элементов, для которых может потребоваться надежная утилизация;

c) может оказаться проще организовать сбор и надежную утилизацию в отношении всех носителей информации, чем пытаться выделить носители с информацией ограниченного доступа;

d) многие организации предлагают услуги по сбору и утилизации носителей; следует уделять особое внимание выбору подходящего подрядчика с учетом имеющегося у него опыта и применяемых адекватных мер обеспечения безопасности;

e) утилизацию носителей, содержащих информацию ограниченного доступа, следует фиксировать как контрольную запись для аудита.

При накоплении носителей, подлежащих утилизации, следует учитывать «эффект накопления», который может стать причиной того, что большое количество информации неограниченного доступа становится доступной.

Дополнительная информация

Для поврежденных устройств, содержащих информацию ограниченного доступа, может потребоваться оценка рисков на предмет того, должны ли эти устройства быть физически уничтожены, а не отправлены в ремонт или выброшены (см. 11.2.7).

**8.3.3 Перемещение физических носителей**

Мера обеспечения ИБ

Во время транспортировки носители информации, содержащие информацию, должны быть защищены от несанкционированного доступа, ненадлежащего использования или повреждения.

Руководство по применению

Для защиты носителей информации, подлежащих транспортировке, должны быть приняты во внимание следующие рекомендации:

a) должен использоваться надежный транспорт или курьеры;

b) перечень авторизованных курьеров должен быть согласован с руководством;

c) должны быть разработаны процедуры для идентификации курьеров;

d) упаковка должна обеспечивать защиту содержимого от любых физических повреждений, которые могут возникнуть в ходе транспортировки, и соответствовать требованиям производителей, например обеспечивать защиту от воздействия любых факторов окружающей среды, которые могут снизить возможность восстановления носителей, таких как тепло, влага или электромагнитные поля;

e) должны регистрироваться записи о содержании носителей, применяемых мерах обеспечения ИБ, а также о времени передачи курьеру для транспортировки и времени получения в пункте назначения.

Дополнительная информация

Информация может быть уязвимой к несанкционированному доступу, нецелевому использованию или повреждению в ходе транспортировки, например при отправке носителя через почтовую службу или курьером. В этом случае носители включают в себя и бумажные документы.

В тех случаях, когда конфиденциальная информация на носителе не зашифрована, следует рассмотреть вопрос о дополнительной физической защите носителя.

## 9 Управление доступом

### 9.1 Требование бизнеса по управлению доступом

| |
|---|
| Цель: Ограничить доступ к информации и средствам ее обработки. |

**9.1.1 Политика управления доступом**

Мера обеспечения ИБ

Политика управления доступом должна быть разработана, документирована и периодически пересматриваться с учетом требований бизнеса и ИБ.

Руководство по применению

Владельцы активов должны определить соответствующие правила управления доступом, права доступа и ограничения для конкретных пользовательских ролей по отношению к своим активам с уровнем детализации и строгостью мер, отражающих риски, связанные с обеспечением ИБ.

Меры по управлению доступом могут быть как логическими, так и физическими (раздел 11), и должны рассматриваться совместно. Пользователи и поставщики услуг должны получить четкое представление о требованиях бизнеса, которым должны удовлетворять меры управления доступом.

Политика должна учитывать следующее:

a) требования безопасности бизнес-приложений;

b) политики распространения информации и авторизации, например принцип «необходимого знания», уровни ИБ и категорирование информации (см. 8.2);

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

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

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

f) разделение ролей по управлению доступом, например запрос доступа, авторизация доступа, администрирование доступа;

g) требования к формальной авторизации запросов доступа (см. 9.2.1 и 9.2.2);

h) требования к периодическому пересмотру прав доступа (см. 9.2.6);

i) аннулирование прав доступа (см. 9.2.6);

j) архивирование записей всех значимых событий, касающихся использования и управления идентификаторами пользователей и секретной аутентификационной информацией;

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

Дополнительная информация

Следует уделять особое внимание установлению правил управления доступом и учитывать следующее:

a) установление правил, основанных на утверждении «Все в общем случае запрещено, пока явно не разрешено», а не на более слабом принципе «Все в общем случае разрешено, пока явно не запрещено»;

b) изменения маркировки информации (см. 8.2.2), которые инициируются автоматически средствами обработки информации и которые инициируются пользователями;

c) изменения в правах пользователей, которые инициируются автоматически информационной системой, и те, которые инициируются администратором;

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

Правила управления доступом должны быть зафиксированы в формальных процедурах (см. 9.2, 9.3, 9.4), и под них определены обязанности (см. 6.1, 9.3).

Управление доступом на основе ролей — это подход, успешно используемый многими организациями для связи прав доступа с бизнес-ролями.

Есть два часто применяемых принципа, определяющих политику управления доступом:

e) принцип «необходимого знания»: вам предоставляется доступ только к той информации, которая вам необходима для выполнения ваших задач (различные задачи/роли подразумевают различные «необходимые знания» и следовательно различные профили доступа);

f) принцип «необходимого использования»: вам предоставляется доступ только к тем средствам обработки информации (ИТ-оборудование, приложения, процедуры, помещения), которые необходимы для выполнения задачи/работы/роли.

**9.1.2 Доступ к сетям и сетевым сервисам**

Мера обеспечения ИБ

Пользователям следует предоставлять доступ только к тем сетям и сетевым сервисам, на использование которых они получили конкретное разрешение.

Руководство по применению

В отношении использования сетей и сетевых сервисов должна быть сформулирована политика. Эта политика должна охватывать:

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

b) процедуры авторизации для определения того, кому к каким сетям и сетевым сервисам разрешен доступ;

c) меры управления и процедуры для защиты доступа к сетевым соединениям и сетевым сервисам;

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

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

f) мониторинг использования сетевых сервисов.

Политика использования сетевых сервисов должна быть согласованной с политикой управления доступом организации (см. 9.1.1).

Дополнительная информация

Несанкционированные и незащищенные подключения к сетевым сервисам могут повлиять на всю организацию. Контроль подключений особенно важен для сетевых подключений к критически важным с точки зрения бизнеса приложениям или для пользователей, находящихся в местах с высоким уровнем риска, например в общественных местах или местах за пределами организации, которые не попадают под контроль системы менеджмента информационной безопасности организации.

### 9.2 Процесс управления доступом пользователей

Цель: Обеспечить предоставление доступа уполномоченным пользователям и предотвратить несанкционированный доступ к системам и сервисам.

#### 9.2.1 Регистрация и отмена регистрации пользователей

Мера обеспечения ИБ

Для назначения прав доступа должна быть реализована формализованная процедура регистрации и отмены регистрации пользователей.

Руководство по применению

Процесс управления идентификаторами пользователей должен включать в себя:

a) использование уникальных идентификаторов пользователей, позволяющих отследить действия пользователей, чтобы они несли ответственность за свои действия; использование групповых идентификаторов должно быть разрешено только в тех случаях, когда это необходимо для бизнеса или в силу операционных причин и должно быть утверждено и документировано;

b) немедленное отключение или удаление идентификаторов пользователей, покинувших организацию (см. 9.2.6);

c) периодическое выявление и удаление или отключение избыточных идентификаторов пользователей;

d) обеспечение того, чтобы избыточные идентификаторы пользователей не были переданы другим пользователям.

Дополнительная информация

Предоставление или аннулирование прав доступа к информации или средствам обработки информации обычно представляет собой двухэтапную процедуру:

a) назначение и активация или аннулирование идентификатора пользователя;

b) предоставление или аннулирование прав доступа для этого идентификатора пользователя (см. 9.2.2).

#### 9.2.2 Предоставление пользователю права доступа

Мера обеспечения ИБ

Должен быть реализован формализованный процесс назначения или отмены прав доступа пользователей к системам и сервисам.

Руководство по применению

Процесс предоставления доступа для назначения или аннулирования прав доступа для идентификаторов пользователей должен включать в себя:

a) получение разрешения от владельца информационной системы или сервиса на использование этой информационной системы или сервиса (см. 8.1.2); также может быть целесообразным разделение подтверждения прав доступа от управления;

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

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

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

e) корректировку прав доступа пользователей, у которых поменялись роли или задачи, а также немедленное удаление или блокирование прав доступа пользователей, покинувших организацию;

f) периодический пересмотр права доступа совместно с владельцами информационных систем или сервисов (см. 9.2.5).

Дополнительная информация

Следует рассмотреть вопрос о создании ролей пользователей, которые вытекают из требований бизнеса и определяют права доступа для пользователей, объединяя ряд прав доступа в типовые профили доступа пользователей. Запросы на доступ и пересмотр прав доступа (см. 9.2.4) легче обрабатывать на уровне таких ролей, чем на уровне отдельных прав.

Следует рассмотреть вопрос включения в контракты с работниками и подрядчиками положений, предусматривающих санкции в случае совершения работником или подрядчиком попыток несанкционированного доступа (см. 7.1.2, 7.2.3, 13.2.4; 15.1.2).

**9.2.3 Управление привилегированными правами доступа**

Мера обеспечения ИБ

Распределение и использование привилегированных прав доступа следует ограничивать и контролировать.

Руководство по применению

Назначение привилегированных прав доступа должно контролироваться посредством формализованного процесса аутентификации в соответствии с действующей политикой управления доступом (см. 9.1.1). При этом должны быть предусмотрены следующие шаги:

a) идентификация привилегированных прав доступа, связанных с каждой системой или процессом, например операционной системой, системой управления базами данных, каждым приложением и пользователями, которым требуется назначение таких прав;

b) привилегированные права доступа должны назначаться пользователям исходя из принципов «необходимого использования» и «предоставления доступа по событию» в соответствии с политикой управления доступом (см. 9.1.1), то есть по минимуму для их функциональных ролей;

c) все процессы аутентификации и назначения привилегий должны регистрироваться. Привилегированные права доступа не должны предоставляться до завершения процесса аутентификации;

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

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

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

g) должны быть разработаны и поддерживаться специальные процедуры, во избежание несанкционированного использования общих административных идентификаторов в соответствии с возможностями конфигурации системы;

h) при совместном использовании общих административных идентификаторов должна обеспечиваться конфиденциальность секретной аутентификационной информации (например, частая смена паролей, а также максимально быстрая их смена при увольнении пользователя с привилегированными правами или изменении его обязанностей, передача паролей всем пользователям с привилегированными правами посредством соответствующих механизмов).

Дополнительная информация

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

**9.2.4 Процесс управления секретной аутентификационной информацией пользователей**

Мера обеспечения ИБ

Предоставление секретной аутентификационной информации должно контролироваться посредством формального процесса управления.

Руководство по применению

Этот процесс должен включать в себя следующие требования:

a) пользователи должны подписывать соглашение о сохранении конфиденциальности личной секретной аутентификационной информации и секретной аутентификационной информации группы (то есть совместно используемой информации) исключительно в пределах группы; это подписанное соглашение может быть включено в правила и условия работы (см. 7.1.2);

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

c) должны быть установлены процедуры для проверки личности пользователя перед предоставлением новой (в том числе временной) секретной аутентификационной информации или заменой старой информации;

d) временная секретная аутентификационная информация должна передаваться пользователю безопасным способом; следует избегать использования третьих сторон или незащищенного (открытого) текста сообщений электронной почты;

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

f) пользователи должны подтвердить получение секретной аутентификационной информации;

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

Дополнительная информация

Пароли являются широко используемым типом секретной аутентификационной информации и распространенным средством проверки подлинности пользователя. Другим типом секретной аутентификационной информации являются криптографические ключи и другие данные, хранящиеся на аппаратных токенах (например, смарт-картах), которые генерируют коды аутентификации.

**9.2.5 Пересмотр прав доступа пользователей**

Мера обеспечения ИБ

Владельцы активов должны регулярно пересматривать права доступа пользователей.

Руководство по применению

При пересмотре прав доступа следует учитывать следующее:

a) права доступа пользователей следует пересматривать как через определенные интервалы времени, так и после любых изменений, таких как повышение или понижение в должности, или увольнение (раздел 7);

b) права доступа пользователя следует пересматривать и переназначать в случае изменения его роли в организации;

c) полномочия для привилегированных прав доступа следует пересматривать чаще;

d) назначенные привилегии необходимо регулярно проверять для обеспечения уверенности в том, что никто не получил привилегий несанкционированным образом;

e) изменения привилегированных учетных записей необходимо регистрировать для периодического анализа.

Дополнительная информация

Эта мера компенсирует возможные недостатки в выполнении мер обеспечения ИБ, приведенных в 9.2.1, 9.2.2, 9.2.6.

**9.2.6 Аннулирование или корректировка прав доступа**

Мера обеспечения ИБ

Права доступа всех работников и внешних пользователей к информации и средствам ее обработки должны быть аннулированы (после их увольнения, истечения срока действия договора или соглашения) либо скорректированы в случае необходимости.

Руководство по применению

После завершения трудовых отношений права доступа пользователя к информации и активам, связанным со средствами обработки информации и сервисов, должны быть удалены или приостановлены. Это определит, нужно ли удалять права доступа. Изменения в должности должны находить отражение в удалении всех прав доступа, которые не были одобрены для новой позиции. Права доступа, которые должны быть удалены или изменены, распространяются также на физический и логический доступ. Удаление или изменение прав доступа могут быть выполнены путем удаления, отзыва или замены ключей, идентификационных карточек, средств обработки информации или абонементов. Любая

документация, определяющая права доступа работников и подрядчиков, должна отражать удаление или изменение прав доступа. Если работнику или внешнему пользователю, прекращающему работу, известны пароли для остающихся активными логинов пользователей, они должны быть изменены после прекращения или изменения трудовых отношений, контракта или соглашения.

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

a) кем было инициировано прекращение или изменение трудовых отношений: работником, сторонним пользователем или руководством, а также причина прекращения отношений;

b) текущие обязанности работника, внешнего пользователя или любого другого пользователя;

c) ценность активов, находящихся в текущем доступе.

Дополнительная информация

В определенных обстоятельствах права доступа могут быть назначены более широкому кругу людей, нежели увольняемые работники или внешние пользователи, например с использованием групповых идентификаторов. В таком случае увольняемые работники должны быть удалены из любого списка группового доступа и должны быть приняты меры, чтобы уведомить всех других работников и внешних пользователей о том, чтобы не передавать более эту информацию лицу, покидающему организацию.

В том случае, когда увольнение инициировано руководством, недовольные работники или внешние пользователи могут намеренно повредить информацию или вывести из строя средства обработки информации. Уволившиеся или уволенные работники могут попытаться скопировать информацию для будущего использования.

### 9.3 Ответственность пользователей

Цель: Установить ответственность пользователей за защиту их аутентификационной информации.

#### 9.3.1 Использование секретной аутентификационной информации

Мера обеспечения ИБ

При использовании секретной аутентификационной информации пользователи должны выполнять установленные в организации правила.

Руководство по применению

Всем пользователям должно быть рекомендовано:

a) хранить секретную аутентификационную информацию в тайне, гарантируя, что она не будет разглашена никакой другой стороне, в том числе представителям органов власти;

b) избегать хранения записей секретной аутентификационной информации (например на бумаге, в файле программного обеспечения или на мобильном устройстве), кроме тех случаев, когда эти записи могут быть надежно сохранены, а способ хранения одобрен (например хранилище паролей);

c) изменять секретную аутентификационную информацию всякий раз, когда есть какие-либо признаки ее возможной компрометации;

d) когда в качестве секретной аутентификационной информации используются пароли, необходимо выбирать стойкие пароли с достаточной минимальной длиной, которые:

1) легко запомнить;

2) не основаны на том, о чем кто-либо другой может легко догадаться или вычислить на основе личной информации, например имена, номера телефонов и даты рождения и т. д.;

3) неуязвимы к атакам по словарю (т. е. не состоят из слов, включенных в словари);

4) не содержат последовательности идентичных символов, не являются полностью цифровыми или буквенными;

5) если являются временными, изменяются при первом входе в систему;

6) не делятся секретной аутентификационной информацией;

7) помогают обеспечить надлежащую защиту в тех случаях, когда пароли используются в качестве секретной аутентификационной информации в процедурах автоматического входа и хранятся в системе;

e) не используют одну и ту же секретную аутентификационную информацию для деловых и частных целей.

Дополнительная информация

Применение технологии единого входа (англ. Single Sign-On, SSO) или других инструментов управления секретной аутентификационной информацией уменьшает объем секретной аутентификационной информации, которую пользователи должны защищать, и, таким образом, может повысить эффективность этой меры обеспечения ИБ. Однако эти инструменты также могут увеличить последствия от раскрытия секретной аутентификационной информации.

### 9.4 Управление доступом к системам и приложениям

Цель: Предотвратить несанкционированный доступ к системам и приложениям.

#### 9.4.1 Ограничение доступа к информации

Мера обеспечения ИБ

Доступ к информации и функциям прикладных систем должен быть ограничен в соответствии с политикой управления доступом.

Руководство по применению

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

Для обеспечения выполнения требований по ограничению доступа следует учитывать следующее:

a) предоставление меню для управления доступом к функциям прикладных систем;

b) управление тем, какие данные могут быть доступны конкретному пользователю;

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

d) управление правами доступа других приложений;

e) ограничение информации, содержащейся в выходных данных;

f) обеспечение физических или логических мер управления доступом для изоляции чувствительных приложений, данных или систем.

#### 9.4.2 Безопасные процедуры входа в систему

Мера обеспечения ИБ

Когда этого требует политика управления доступом, доступ к системам и приложениям должен управляться посредством безопасной процедуры входа в систему.

Руководство по применению

Должны быть выбраны подходящие методы аутентификации для подтверждения заявленной личности пользователя.

Там, где требуется строгая аутентификация и проверка личности, должны использоваться методы аутентификации, альтернативные паролям, такие как криптографические средства, смарт-карты, токены или биометрические средства.

Процедура входа в систему или приложение должна быть разработана таким образом, чтобы минимизировать возможность несанкционированного доступа. Таким образом, процедура входа в систему должна раскрывать минимум информации о системе или приложении, во избежание оказания какой-либо неумышленной помощи неавторизованному пользователю. Разработанная надлежащим образом процедура входа должна:

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

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

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

d) осуществлять подтверждение информации для входа только после завершения ввода всех данных. Если возникает ошибка, система не должна указывать, какая часть данных для входа является правильной или неправильной;

e) защищать от попыток входа в систему методом полного перебора (грубой силы);

f) регистрировать неуспешные и успешные попытки входа;

g) фиксировать событие безопасности при обнаружении попыток или фактов успешного нарушения процедуры входа;

h) отображать следующую информацию по завершении успешного входа в систему:
- дата и время предыдущего успешного входа;
- сведения всех неудачных попыток входа с момента последнего успешного входа;

i) не отображать вводимый пароль;

j) не передавать пароли в открытом виде по сети;

k) завершать неактивные сессии после определенного периода бездействия, особенно в местах повышенного риска, таких как общественные места или точки за пределами организации, которые не попадают под контроль системы менеджмента информационной безопасности организации, или на мобильных устройствах;

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

Дополнительная информация

Пароли являются наиболее распространенным способом обеспечения идентификации и аутентификации на основе использования секрета, который знает только пользователь. То же самое может быть достигнуто при использовании криптографических средств и протоколов аутентификации. Надежность аутентификации пользователя должна соответствовать категории информации, к которой осуществляется доступ.

Если пароли передаются по сети в открытом виде во время процедуры входа, они могут быть перехвачены программой анализа сетевого трафика.

**9.4.3 Система управления паролями**

Мера обеспечения ИБ

Системы управления паролями должны быть интерактивными и должны обеспечивать уверенность в качестве паролей.

Руководство по применению

Система управления паролями должна:

a) обеспечить использование индивидуальных пользовательских идентификаторов и паролей для обеспечения отслеживаемости;

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

c) обеспечивать выбор качественных паролей;

d) заставлять пользователей изменять свои пароли при первом входе в систему;

e) агитировать регулярно или по мере необходимости менять пароли;

f) вести учет ранее использованных паролей и предотвращать их повторное использование;

g) не отображать пароли на экране при их вводе;

h) хранить файлы с паролями отдельно от данных прикладных систем;

i) хранить и передавать пароли в защищенном виде.

Дополнительная информация

Некоторые приложения требуют, чтобы пароли пользователей назначались независимой стороной; в таких случаях пункты b), d) и e) вышеуказанного руководства к системе не применяются. В большинстве случаев пароли выбирают и меняют пользователи.

**9.4.4 Использование привилегированных служебных программ**

Мера обеспечения ИБ

Использование служебных программ, которые могли бы обойти меры и средства ИБ систем и приложений, следует ограничивать и строго контролировать.

Руководство по применению

Следует учитывать следующие рекомендации по использованию служебных программ, которые могут обходить меры обеспечения ИБ систем и прикладных программ:

a) использовать процедуры идентификации, аутентификации и авторизации для служебных программ;

b) отделять служебные программы от прикладного программного обеспечения;

c) ограничивать использование служебных программ минимально возможным числом доверенных, авторизованных пользователей (см. 9.2.3);

d) предъявлять требования по авторизации на использование специальных служебных программ;

e) ограничивать доступность системных служебных программ, например на время внесения авторизованных изменений;

f) регистрировать все случаи использования служебных программ;

g) определять и документировать уровни авторизации для служебных программ;

h) удалять или отключать все ненужные служебные программы;

i) не делать служебные программы доступными тем пользователям, которые имеют доступ к прикладным программам в системах, где требуется разделение обязанностей.

Дополнительная информация

Большинство компьютеров имеют, как правило, одну или несколько служебных программ, способных обойти меры обеспечения ИБ эксплуатируемых систем и прикладных программ.

**9.4.5 Управление доступом к исходному коду программы**

Мера обеспечения ИБ

Доступ к исходному коду программ должен быть ограничен.

Руководство по применению

Доступ к исходному коду программы и связанным с ним элементам (таким, как проекты, спецификации, планы верификации и валидации) должен строго контролироваться для того, чтобы предотвратить внедрение в него несанкционированного функционала и избежать непреднамеренных изменений, а также сохранить конфиденциальность ценной интеллектуальной собственности. Для исходного кода программы это может быть достигнуто путем контролируемого централизованного хранения такого кода, предпочтительно в библиотеках исходных кодов программ. Затем следует учесть следующие рекомендации для управления доступом к таким библиотекам исходных кодов программ для того, чтобы уменьшить вероятность повреждения компьютерных программ:

a) где это возможно, библиотеки исходных кодов программ не должны содержаться в эксплуатируемых системах;

b) исходный код программы и библиотеки исходных кодов программы должны управляться в соответствии с установленными процедурами;

c) вспомогательный персонал не должен иметь неограниченный доступ к библиотекам исходных кодов программы;

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

e) листинги программ должны храниться в безопасной среде;

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

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

Если исходный код программы предполагается публиковать, следует принять во внимание дополнительные меры обеспечения ИБ для получения гарантии его целостности (например, электронная подпись).

## 10 Криптография[1)]

### 10.1 Средства криптографической защиты информации

Цель: Обеспечить уверенность в надлежащем и эффективном использовании криптографии для защиты конфиденциальности, подлинности (аутентичности) и/или целостности информации.

**10.1.1 Политика использования средств криптографической защиты информации**

Мера обеспечения ИБ

Должна быть разработана и внедрена политика использования средств криптографической защиты информации.

Руководство по применению

При разработке политики следует учитывать следующее:

a) подход к управлению применением средств криптографической защиты информации в организации, включая главные принципы, на которых должна быть основана защита коммерческой информации;

---

[1)] Применение криптографических методов защиты информации осуществляется в соответствии с законодательством Российской Федерации.

b) определенный на основе оценки риска требуемый уровень защиты с учетом типа, стойкости и качества требуемого алгоритма шифрования;

c) использование шифрования для защиты информации, передаваемой с помощью мобильных или съемных носителей, или по линиям связи;

d) подход к управлению ключами, в том числе методы по защите криптографических ключей и восстановлению зашифрованной информации в случае утери, компрометации или повреждения ключей;

e) роли и обязанности, например, кто несет ответственность за:

1) внедрение политики;

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

f) стандарты, которые должны быть приняты для эффективной реализации во всей организации (какое решение используется и для каких бизнес-процессов);

g) влияние использования зашифрованной информации на меры обеспечения ИБ, которые базируются на проверке содержимого (например, обнаружение вредоносного ПО).

При внедрении политики криптографической защиты в организации следует учитывать требования законодательства и ограничения, которые могут применяться в отношении использования криптографических методов в разных странах, а также вопросы трансграничной передачи зашифрованной информации (см. 18.1.5).

Средства криптографической защиты информации могут использоваться для достижения различных целей, например:

a) обеспечение конфиденциальности: использование шифрования для защиты информации ограниченного доступа как при хранении, так и при передаче;

b) обеспечение целостности и аутентичности: использование электронных подписей или кодов аутентификации сообщений для проверки подлинности или целостности информации ограниченного доступа при ее передаче и хранении;

c) обеспечение неотказуемости: использование криптографических методов для подтверждения наличия или отсутствия события или действия;

d) аутентификация: использование криптографических методов для аутентификации пользователей и других системных объектов, запрашивающих доступ к пользователям, объектам и ресурсам системы или осуществляющих операции с ними.

Дополнительная информация

Принятие решения о применении криптографических решений следует рассматривать как часть более широкого процесса оценки риска и выбора мер обеспечения ИБ. Такая оценка может затем использоваться для определения того, является ли криптографическая мера подходящей, какой тип мер следует применять, с какой целью и для каких бизнес-процессов.

Политика использования криптографических мер необходима для достижения максимальных выгод и минимизации рисков использования криптографических мер, а также во избежание ненадлежащего или неправильного их использования.

Следует проконсультироваться со специалистами при выборе подходящих средств криптографической защиты информации для достижения целей политики ИБ.

**10.1.2 Управление ключами**

Мера обеспечения ИБ

Политика, определяющая использование, защиту и срок действия криптографических ключей, должна быть разработана и применяться на протяжении всего их жизненного цикла.

Руководство по применению

Политика должна включать требования к управлению криптографическими ключами на протяжении всего их жизненного цикла, включая генерацию, хранение, архивирование, получение, распространение, удаление и уничтожение ключей.

Криптографические алгоритмы, длина ключей и методы использования должны выбираться исходя из лучших практик. Надлежащее управление ключами требует безопасных процессов генерации, хранения, архивирования, извлечения, распространения, удаления и уничтожения криптографических ключей.

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

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

a) генерации ключей для различных криптографических систем и приложений;

b) выдачи и получения сертификатов открытого ключа;

c) распределения ключей тем, кому они предназначены, в том числе порядок активации ключей при получении;

d) хранения ключей, в том числе того, как авторизованные пользователи получают доступ к ключам;

e) смены или обновления ключей, включая руководство о том, когда следует менять ключи и как это сделать;

f) действий со скомпрометированными ключами;

g) отзыва ключей, в том числе того, как ключи должны быть аннулированы или деактивированы, например, когда ключи были скомпрометированы, или когда пользователь покидает организацию (в этом случае ключи также должны быть архивированы);

h) восстановления поврежденных и утерянных ключей;

i) резервного копирования или архивирования ключей;

j) уничтожения ключей;

k) регистрации и аудита действий по управлению ключами.

В политике управления ключами следует определить даты активации и деактивации ключей, чтобы ключи могли использоваться только в течение периода времени, что уменьшит вероятность их ненадлежащего использования.

В дополнение к вопросу безопасного управления секретными и закрытыми ключами следует также учитывать вопросы аутентичности открытых ключей. Процесс аутентификации достигается применением сертификатов открытых ключей, которые обычно выдаются удостоверяющим центром — признанной организацией с соответствующими реализованными мерами и процедурами для обеспечения требуемого уровня доверия.

Содержание соглашений об уровне обслуживания или договоров с внешними поставщиками криптографических услуг, например с удостоверяющим центром, должно охватывать вопросы ответственности, надежности услуг и времени реагирования на запросы (см. 15.2).

Дополнительная информация

Управление криптографическими ключами имеет важное значение для эффективного использования криптографических методов. ИСО/МЭК 11770 [2], [3], [4] предоставляет дополнительную информацию об управлении ключами.

Криптографические методы также могут быть использованы для защиты криптографических ключей. Возможно, потребуется наличие процедур по обработке запросов от правоохранительных органов на доступ к криптографическим ключам, например зашифрованная информация может потребоваться в незашифрованном виде в качестве доказательства в суде.

## 11 Физическая безопасность и защита от воздействия окружающей среды

### 11.1 Зоны безопасности

Цель: Предотвратить несанкционированный физический доступ, повреждение и воздействие на информацию организации и средства ее обработки.

#### 11.1.1 Физический периметр безопасности

Мера обеспечения ИБ

Должны быть определены и использованы периметры безопасности для защиты зон, содержащих информацию ограниченного доступа и средства ее обработки.

Руководство по применению

Там, где это применимо, для физических периметров безопасности должны быть рассмотрены и реализованы следующие рекомендации:

a) периметры безопасности должны быть четко определены, а расположение и степень защиты каждого из них должны зависеть от требований безопасности активов в пределах периметра и результатов оценки риска;

b) периметры здания или помещения, где расположены средства обработки информации, должны быть физически прочными (то есть не должно быть пробелов по периметру или участков, где можно

легко проникнуть); внешняя крыша, стены и полы помещений должны быть надлежащим образом защищены от несанкционированного доступа с помощью соответствующих механизмов (например, решеток, сигнализации, замков); двери и окна должна быть заперты, когда они находятся без присмотра, и следует рассмотреть вопрос внешней защиты окон, особенно если они находятся на уровне земли;

c) для контроля физического доступа в здание или помещение должна быть выделена и укомплектована персоналом зона приема посетителей или предусмотрены другие меры контроля; доступ в помещения и здания должен быть предоставлен только авторизованному персоналу;

d) где это применимо, должны быть установлены физические барьеры для предотвращения несанкционированного доступа и воздействия окружающей среды;

e) все пожарные выходы по периметру безопасности должны безотказно функционировать в соответствии с местными правилами пожарной безопасности, быть оборудованы аварийной сигнализацией, находиться под наблюдением и проверены в местах соединения со стенами для установления необходимого уровня защищенности в соответствии с действующими региональными, национальными и международными стандартами;

f) следует установить подходящие системы обнаружения вторжений в соответствии с национальными, региональными или международными стандартами, а также регулярно их проверять, покрывая при этом все доступные снаружи двери и окна; незанятые площади должны быть поставлены на постоянную сигнализацию; аналогично следует оборудовать и другие зоны, например серверную или кроссовую;

g) средства обработки информации, которыми управляет организация, должны быть физически отделены от средств, управляемых сторонними организациями.

Дополнительная информация

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

Зоной безопасности может быть запираемый офис или несколько помещений, окруженных непрерывным внутренним физическим барьером. Могут потребоваться дополнительные барьеры и периметры для контроля физического доступа между зонами с различными требованиями безопасности. Особое внимание безопасности физического доступа должно быть уделено в случае, если в здании находятся активы нескольких организаций.

Применение мер обеспечения физической безопасности, особенно в зонах безопасности, должно быть адаптировано к техническому и экономическому положению организации, как это следует из оценки рисков.

**11.1.2 Меры и средства контроля и управления физическим доступом**

Мера обеспечения ИБ

Зоны безопасности должны быть защищены соответствующими мерами и средствами контроля доступа, чтобы обеспечить уверенность в том, что доступ разрешен только уполномоченному персоналу.

Руководство по применению

Следует принять во внимание следующие рекомендации:

a) регистрировать дату и время въезда и выезда посетителей, а также брать под сопровождение всех, чье право доступа не было предварительно согласовано; доступ посетителям следует предоставлять только для выполнения определенных, авторизованных целей и следует начинать с проведения инструктажа по требованиям безопасности и действий в аварийных ситуациях. Личность посетителей должна подтверждаться соответствующими средствами;

b) доступ в зоны обработки или хранения конфиденциальной информации следует контролировать и предоставлять только авторизованным лицам путем применения соответствующих мер, например реализацией механизма двухфакторной аутентификации, такой, как карты доступа или секретным ПИН-кодом;

c) рукописный или электронный журнал регистрации посещений нужно надежным образом вести и проверять;

d) все работники, подрядчики и представители внешней стороны должны носить ту или иную форму визуального идентификатора и должны немедленно уведомлять персонал службы безопасности, если они встречают посетителей без сопровождения или без визуальных идентификаторов;

e) персоналу службы поддержки сторонних организаций следует выдавать ограниченный доступ к зонам и средствам обработки конфиденциальной информации только при необходимости; такой доступ должен быть санкционирован и сопровождаться соответствующим контролем;

f) права доступа к зонам безопасности следует регулярно пересматривать и обновлять, а при необходимости отменять (см. 9.25, 9.2.6).

**11.1.3 Безопасность зданий, помещений и оборудования**

Мера обеспечения ИБ

Должна быть разработана и реализована физическая защита зданий, помещений и оборудования.

Руководство по применению

Должны быть рассмотрены следующие рекомендации для обеспечения безопасности зданий, помещений и оборудования:

a) ключевое оборудование должно быть расположено таким образом, чтобы исключить доступ посторонних лиц;

b) где это применимо, здания должны быть неприметными и давать минимальную информацию о своем назначении, без каких-либо явных признаков, как снаружи, так и внутри, определяющих наличие действий по обработке информации;

c) оборудование должно быть настроено так, чтобы конфиденциальная информация или действия по обработке информации не были видны и слышны извне. В отдельных случаях следует рассмотреть электромагнитное экранирование;

d) справочники и внутренние телефонные книги, определяющие местонахождение средств обработки конфиденциальной информации, не должны быть легко доступны для посторонних лиц.

**11.1.4 Защита от внешних угроз и угроз со стороны окружающей среды**

Мера обеспечения ИБ

Должны быть разработаны и реализованы меры физической защиты от стихийных бедствий, злоумышленных атак или аварий.

Руководство по применению

Следует проконсультироваться со специалистом о том, как избежать ущерба от пожара, наводнения, землетрясения, взрыва и других форм стихийных или техногенных бедствий, а также от общественных беспорядков.

**11.1.5 Работа в зонах безопасности**

Мера обеспечения ИБ

Должны быть разработаны и применены процедуры для работы в зонах безопасности.

Руководство по применению

Следует принять во внимание следующие рекомендации:

a) о существовании зоны безопасности и деятельности в ней персонал должен быть осведомлен по «принципу необходимого знания»;

b) следует избегать работ без надлежащего контроля в зонах безопасности, как по соображениям безопасности, так и для предотвращения возможности совершения злонамеренных действий;

c) незанятые зоны безопасности должны быть физически заперты и периодически проверяться;

d) использование фото-, видео-, аудио- и другого записывающего оборудования, такого как камеры в мобильных устройствах, должно быть запрещено без соответствующего на то разрешения.

Меры по работе в зонах безопасности включают в себя меры обеспечения ИБ для работников и представителей внешней стороны, работающих в зоне безопасности, и охватывают все виды деятельности, выполняемые в зоне безопасности.

**11.1.6 Зоны погрузки и разгрузки**

Мера обеспечения ИБ

Места доступа, например зоны погрузки и разгрузки, и другие места, где неуполномоченные лица могут проникать в помещения, должны находиться под контролем и, по возможности, должны быть изолированы от средств обработки информации во избежание несанкционированного доступа к ним.

Руководство по применению

Следует принять во внимание:

a) доступ к зоне погрузки и разгрузки снаружи здания разрешен только идентифицированному и авторизованному персоналу;

b) зона погрузки и разгрузки должна быть спроектирована таким образом, чтобы можно было загружать и выгружать материальные ценности так, чтобы занимающийся этим персонал не имел доступа к другим частям здания;

c) внешние двери зоны погрузки и разгрузки должны быть закрыты в то время, когда внутренние открыты;

d) поступающие материальные ценности должны быть осмотрены и проверены на наличие взрывчатых веществ, химикатов или других опасных материалов, прежде чем они будут перемещены из зоны погрузки и разгрузки;

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

f) где это возможно, получаемые и отправляемые грузы должны быть физически разделены;

g) полученные материальные ценности должны быть осмотрены на предмет наличия следов вскрытия и порчи в пути и, если такое вмешательство было обнаружено, об этом следует немедленно сообщить персоналу службы безопасности.

### 11.2 Оборудование

Цель: Предотвратить потерю, повреждение, хищение или компрометацию активов и прерывание деятельности организации.

#### 11.2.1 Размещение и защита оборудования

Мера обеспечения ИБ

Оборудование должно быть размещено и защищено таким образом, чтобы снизить риски ИБ от угроз и опасностей со стороны окружающей среды и возможности несанкционированного доступа.

Руководство по применению

Следующие рекомендации необходимо рассмотреть для защиты оборудования:

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

b) средства обработки информации, обрабатывающие информацию ограниченного доступа, должны располагаться так, чтобы снизить риск просмотра информации посторонними лицами во время их использования;

c) оборудование для хранения информации следует защищать от несанкционированного доступа;

d) отдельные элементы оборудования, требующие специальной защиты, следует охранять для снижения общего уровня требуемой защиты;

e) должны быть предприняты меры по снижению риска потенциальных физических и природных угроз, например краж, пожаров, взрывов, задымления, затопления (или сбоя в водоснабжении), пыли, вибраций, химических воздействий, перебоев в электроснабжении и связи, электромагнитного излучения и вандализма;

f) должны быть установлены правила по приему пищи, питью и курению вблизи средств обработки информации;

g) следует проводить мониторинг условий окружающей среды, которые могут отрицательно повлиять на работу средств обработки информации, например температура и влажность;

h) внешняя молниезащита должна быть установлена на всех зданиях, а фильтры молниезащиты должны ставиться на всех входящих силовых и коммуникационных линиях;

i) в отношении оборудования, расположенного в промышленных условиях, следует использовать специальные методы защиты, такие как защитные пленки для клавиатуры;

j) оборудование, обрабатывающее конфиденциальную информацию, должно быть защищено соответствующим образом для минимизации риска утечки информации из-за электромагнитного излучения.

#### 11.2.2 Вспомогательные услуги

Мера обеспечения ИБ

Оборудование должно быть защищено от сбоев электропитания и других сбоев, вызванных отказами в предоставлении вспомогательных услуг.

Руководство по применению

Вспомогательные услуги (например, электричество, телекоммуникации, водоснабжение, газ, канализация, вентиляция и кондиционирование) должны:

a) соответствовать спецификациям производителя оборудования и местным законодательным требованиям;

b) регулярно оцениваться на предмет способности соответствовать развитию бизнеса и взаимодействию с другими вспомогательными услугами;

c) регулярно осматриваться и проверяться для обеспечения гарантии их надлежащего функционирования;

d) при необходимости быть оборудованы сигнализацией для выявления неисправностей;

e) при необходимости иметь несколько каналов, физически отделенных друг от друга.

Должны быть обеспечены аварийное освещение и связь. Аварийные выключатели и вентили для отключения питания, воды, газа и других услуг должны быть расположены рядом с аварийными выходами или помещениями с оборудованием.

Дополнительная информация

Дополнительная избыточность сетевых соединений может быть обеспечена получением нескольких каналов связи от более чем одного поставщика услуг.

**11.2.3 Безопасность кабельной сети**

Мера обеспечения ИБ

Кабели питания и телекоммуникационные кабели, используемые для передачи данных или для поддержки информационных сервисов, должны быть защищены от перехвата информации, помех или повреждения.

Руководство по применению

Для обеспечения безопасности кабельной сети следует рассмотреть следующие рекомендации:

a) телекоммуникационные линии и линии питания средств обработки информации, где это возможно, должны находиться под землей или же иметь адекватную альтернативную защиту;

b) силовые кабели должны быть проложены отдельно от телекоммуникационных для предотвращения помех;

c) для информации ограниченного доступа следует рассмотреть дополнительные меры обеспечения ИБ, а именно:

1) использование защищенных кабель-каналов, а также закрываемых помещений или шкафов в точках входа/выхода и коммутации кабелей;
2) использование электромагнитной защиты кабелей;
3) проведение технической экспертизы и физического осмотра несанкционированно подключенных к кабелям устройств;
4) контроль доступа к коммутационным панелям и кабельным помещениям.

**11.2.4 Техническое обслуживание оборудования**

Мера обеспечения ИБ

Необходимо проводить надлежащее техническое обслуживание оборудования для обеспечения его непрерывной доступности и целостности.

Руководство по применению

Необходимо рассмотреть следующие рекомендации в отношении обслуживания оборудования:

a) оборудование следует обслуживать в соответствии с рекомендованной поставщиком периодичностью и спецификациями;

b) техническое обслуживание и ремонт оборудования должен проводить только авторизованный персонал;

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

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

e) должны соблюдаться все требования к техническому обслуживанию, установленные страховыми полисами;

f) перед возвращением оборудования в эксплуатацию после технического обслуживания необходимо осмотреть его, чтобы убедиться, что оборудование не повреждено и нормально функционирует.

**11.2.5 Перемещение активов**

Мера обеспечения ИБ

Вынос оборудования, информации или программного обеспечения за пределы площадки эксплуатации без предварительного разрешения необходимо исключить.

Руководство по применению

Следует рассмотреть следующие рекомендации:

a) должны быть идентифицированы работники и внешние пользователи, которые имеют полномочия разрешать вынос активов за пределы организации;

b) должны быть установлены сроки возврата активов, а после возвращения проверено их соблюдение;

c) когда это необходимо и целесообразно, следует регистрировать вынос и возврат активов;

d) личность, должность и принадлежность лица, которое обрабатывает или использует активы, должны быть задокументированы, и эта документация должна быть возвращена вместе с оборудованием, информацией или программным обеспечением.

Дополнительная информация

Выборочные проверки, проводимые для выявления случаев несанкционированного выноса активов, могут выполняться для выявления несанкционированных записывающих устройств, оружия и так далее, а также для предотвращения их проноса и выноса с территории организации. Такие выборочные проверки должны проводиться в соответствии с действующим законодательством и регламентами. Работники должны быть осведомлены о том, что проводятся выборочные проверки, а эти проверки должны проводиться только в строгом соответствии с требованиями законодательства и регламентов.

**11.2.6 Безопасность оборудования и активов вне помещений организации**

Мера обеспечения ИБ

Следует обеспечивать безопасность активов вне помещений организации, учитывая различные риски ИБ, связанные с работой вне помещений организации.

Руководство по применению

Использование за пределами организации любого оборудования для хранения и обработки информации должно быть разрешено руководством. Это относится как к оборудованию, принадлежащему организации, так и к оборудованию, принадлежащему частным лицам, но используемому от имени организации.

Следует рассмотреть следующие рекомендации для защиты оборудования вне организации:

a) оборудование и носители, вынесенные за пределы помещений организации, не следует оставлять без присмотра в общественных местах;

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

c) меры обеспечения информационной безопасности для работы за пределами организации, например для работы дома, удаленной работы и работы на временных точках, должны определяться на основе оценки риска и применяться в зависимости от ситуации, например запираемые шкафы для документов, политика чистого стола, управление доступом к компьютерам и защищенная связь с офисом (см. также ИСО/МЭК 27033 [15], [16], [17], [18], [19]);

d) когда оборудование, эксплуатируемое за пределами организации, передается между разными лицами или внешними сторонами, следует вести журнал, в котором необходимо фиксировать всю цепочку передачи для оборудования, включая, как минимум, ФИО лица и наименование организации, ответственных за оборудование.

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

Дополнительная информация

Оборудование для хранения и обработки информации включает в себя все виды персональных компьютеров, органайзеров, мобильных телефонов, смарт-карт, документы на бумажных или других носителях, которые предназначены для работы на дому или которые можно выносить с обычного места работы.

Более подробную информацию о других аспектах защиты переносного оборудования можно найти в 6.2.

Возможно, будет целесообразно предотвратить риск, отговорив определенных работников работать вне офиса или ограничив использование ими портативного ИТ-оборудования.

**11.2.7 Безопасная утилизация или повторное использование оборудования**

Мера обеспечения ИБ

Все компоненты оборудования, содержащие носители данных, необходимо проверять с целью обеспечения уверенности, что вся защищаемая информация и лицензионное программное обеспечение были удалены или перезаписаны безопасным образом до утилизации или повторного использования этих компонентов оборудования.

Руководство по применению

Оборудование должно быть проверено на предмет наличия или отсутствия устройства хранения данных перед его утилизацией или повторным использованием.

Носители, содержащие конфиденциальную информацию или информацию, защищенную авторским правом, должны быть физически уничтожены, или информация на них должна быть уничтожена, удалена или перезаписана с использованием методов, позволяющих сделать исходную информацию недоступной для восстановления, в отличие от использования стандартных функций удаления или форматирования.

Дополнительная информация

Для сломанного оборудования, содержащего устройства хранения данных, может потребоваться оценка риска, чтобы определить, должно ли это оборудование быть физически уничтожено, а не отправлено в ремонт или выброшено. Информация может быть скомпрометирована из-за ненадлежащей утилизации или повторного использования оборудования.

Кроме безопасной очистки диска, шифрование диска снижает риск раскрытия конфиденциальной информации в тех случаях, когда оборудование подлежит утилизации или повторному использованию при условии, что:

a) шифрование достаточно стойкое и охватывает весь диск (включая свободное место, файлы подкачки и т. д.);

b) ключи шифрования достаточно длинные, чтобы противостоять атакам методом полного перебора (грубой силы);

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

Для получения дополнительной информации о шифровании см. раздел 10.

Методы надежной перезаписи устройств хранения данных отличаются в зависимости от технологии, применяемой в устройствах хранения. Необходимо проверить, чтобы инструменты для перезаписи были применимы к конкретной технологии.

**11.2.8 Оборудование, оставленное пользователем без присмотра**

Мера обеспечения ИБ

Пользователи должны обеспечить соответствующую защиту оборудования, оставленного без присмотра.

Руководство по применению

Все пользователи должны быть осведомлены о требованиях безопасности и процедурах по защите оборудования, оставленного без присмотра, а также об их обязанностях по реализации такой защиты. Пользователям следует рекомендовать:

a) прерывать активные сессии после завершения работы, если только они не могут быть защищены соответствующим механизмом блокировки, например защищенной паролем заставкой;

b) выходить из приложений или сетевых сервисов, когда в них больше нет необходимости;

c) защищать компьютеры или мобильные устройства от несанкционированного использования с помощью запирания на ключ или с помощью аналогичной меры, например защита устройства паролем, когда оно не используется.

**11.2.9 Политика «чистого стола» и «чистого экрана»**

Мера обеспечения ИБ

Должна быть принята политика «чистого стола» в отношении бумажных документов и сменных носителей информации, а также политика «чистого экрана» для средств обработки информации.

Руководство по применению

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

a) информация ограниченного доступа для бизнеса, например информация на бумажных или электронных носителях, должна быть заперта (в идеале, в сейфе, шкафу или другой мебели, обеспечивающей безопасность), пока она не используется, особенно когда в офисе никого нет;

b) компьютеры и терминалы, оставленные без присмотра, следует оставлять в состоянии выполненного выхода из системы или защиты механизмом блокировки экрана и клавиатуры, управляемым паролем, аппаратным ключом или подобным средством аутентификации пользователя, и они должны быть заперты на ключ, защищены паролем или иными мерами, когда не используются;

c) следует предотвращать несанкционированное использование копировальных аппаратов и других воспроизводящих устройств (например, сканеров, цифровых камер);

d) носители, содержащие информацию ограниченного доступа, следует забирать из принтеров немедленно.

Дополнительная информация

Политика «чистого стола» и «чистого экрана» снижает риски несанкционированного доступа, потери и повреждения информации в рабочее и внерабочее время. Сейфы или другие виды защищенных хранилищ могут также защищать хранящуюся в них информацию от таких угроз, как пожар, землетрясение, наводнение или взрыв.

Следует рассмотреть возможность использовании принтеров с функцией PIN-кода, чтобы только создатели документа могли получать его распечатки, находясь непосредственно у принтера.

## 12 Безопасность при эксплуатации

### 12.1 Эксплуатационные процедуры и обязанности

| |
|---|
| Цель: Обеспечить надлежащую и безопасную эксплуатацию средств обработки информации. |

#### 12.1.1 Документально оформленные эксплуатационные процедуры

Мера обеспечения ИБ

Эксплуатационные процедуры должны быть документированы и доступны всем нуждающимся в них пользователям.

Руководство по применению

Должны быть разработаны эксплуатационные процедуры для повседневной деятельности, связанной со средствами обработки информации и связи, такими как процедуры включения и выключения компьютеров, резервного копирования, обслуживания оборудования, обращения с носителями, управления и обеспечения безопасности в серверной комнате и при обработке почты.

Эксплуатационные процедуры должны содержать инструкции, в том числе:

a) по установке и настройке систем;

b) по обработке информации как в автоматизированном, так и в ручном режиме;

c) по резервному копированию (см. 12.3);

d) по требованиям к графику работы, включая взаимосвязь между системами, самое раннее время начала работы и самое позднее время завершения работы;

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

f) контакты поддержки (включая внешнюю) и эскалации на случай непредвиденных эксплуатационных или технических трудностей;

g) инструкции по обращению с особыми носителями и выводом данных, такие как использование специальной бумаги или управление выводом конфиденциальной информации, включая процедуры по безопасному удалению результатов вывода в случае сбоя в работе (см. 8.3 и 11.2.7);

h) процедуры перезапуска и восстановления системы в случае сбоя;

i) управления информацией системных журналов и журналов аудита (см. 12.4);

j) процедуры мониторинга.

Эксплуатационные процедуры и документированные процедуры по системным операциям должны рассматриваться как официальные документы и вносимые в них изменения должны утверждаться руководством. Там, где это технически возможно, информационные системы должны управляться единообразно, с использованием одних и тех же процедур, инструментов и служебных программ.

#### 12.1.2 Процесс управления изменениями

Мера обеспечения ИБ

Необходимо обеспечить управление изменениями в организации, бизнес-процессах, средствах обработки информации и системах, влияющих на ИБ.

Руководство по применению

В частности, необходимо принять во внимание следующее:

a) идентификацию и регистрацию существенных изменений;

b) планирование и тестирование изменений;

c) оценку потенциального влияния от реализации существенных изменений, включая влияние на ИБ;

d) процедуры утверждения предлагаемых изменений;

e) подтверждение того, что выполняются требования по ИБ;

f) информирование об изменении всех заинтересованных лиц;

g) процедуры по возврату в исходное состояние, включая процедуры и обязанности по прерыванию процесса и последующего восстановления после неудачных изменений и непредвиденных событий;

h) установление процесса экстренного изменения для обеспечения быстрой и управляемой реализации изменений, необходимых для разрешения инцидента (см. 16.1).

С целью обеспечения уверенности в надлежащем контроле всех изменений должна быть формально определена ответственность и разработаны соответствующие процедуры управления. При внесении изменений вся необходимая информация должна быть сохранена в контрольном журнале.

Дополнительная информация

Неадекватный контроль над изменениями в средствах и системах обработки информации является распространенной причиной системных сбоев или нарушений безопасности (см. 14.2.2).

**12.1.3 Управление производительностью**

Мера обеспечения ИБ

Необходимо осуществлять мониторинг, корректировку и прогнозирование использования ресурсов исходя из будущих требований к производительности, для обеспечения требуемой производительности системы.

Руководство по применению

Требования к производительности должны быть определены с учетом важности рассматриваемой системы для бизнеса. Необходимо проводить настройку и мониторинг системы для гарантии и, где это применимо, повышения доступности и эффективности системы. Для своевременного выявления проблем следует задействовать соответствующие средства обнаружения. Прогнозирования требований к производительности должны учитывать новые требования как со стороны бизнеса, так и со сторон систем, а также текущие и будущие тенденции в возможностях обработки информации в организации.

Особое внимание следует уделять ресурсам, требующим длительного времени на закупку или высоких затрат, поэтому руководители должны следить за использованием ключевых системных ресурсов. Они должны определять тенденции использования, особенно в отношении бизнес-приложений или инструментов управления информационными системами.

Руководители должны использовать эту информацию для выявления зависимости от основных работников и предотвращения потенциальных узких мест, которые могут представлять угрозу безопасности систем или сервисов, а также планирования соответствующего действия.

Обеспечение достаточного уровня производительности может быть достигнуто как путем наращивания мощностей, так и снижением спроса. Примеры мер снижения спроса включают в себя:

a) удаление устаревших данных (дисковое пространство);

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

c) оптимизацию пакетных заданий и расписаний;

d) оптимизацию логики приложения или запросов к базе данных;

e) запрет или ограничение полосы пропускания для ресурсоемких сервисов, если они не являются критически важными для бизнеса (например, потоковое видео).

В отношении критически важных систем следует иметь задокументированный план управления производительностью.

Дополнительная информация

Данная мера обеспечения ИБ также применима к человеческим ресурсам, а также к помещениям и оборудованию.

**12.1.4 Разделение сред разработки, тестирования и эксплуатации**

Мера обеспечения ИБ

Для снижения рисков несанкционированного доступа или изменений среды эксплуатации необходимо обеспечивать разделение сред разработки, тестирования и эксплуатации.

Руководство по применению

Должен быть определен и реализован необходимый для предотвращения эксплуатационных проблем уровень разделения среды разработки, тестирования и эксплуатации.

Необходимо принять во внимание следующие пункты:

a) правила перевода программного обеспечения из состояния разработки в состояние эксплуатации должны быть определены и задокументированы;

b) программное обеспечение для разработки и эксплуатации должно быть развернуто на разных системах или компьютерах и в разных доменах или каталогах;

c) изменения в эксплуатируемых системах и приложениях должны быть протестированы в тестовой или промежуточной среде перед их применением;

d) кроме как при возникновении исключительных ситуаций, тестирование не должно проводиться на эксплуатируемой среде;

e) компиляторы, редакторы и другие средства разработки или системные служебные программы не должны быть доступны из среды эксплуатации без необходимости;

f) пользователи должны использовать разные профили для сред эксплуатации и тестирования, а на экране должны отображаться соответствующие предупреждающие сообщения, чтобы снизить риск ошибки;

g) конфиденциальные данные не должны копироваться в среду системы тестирования, если для системы тестирования не предусмотрены эквивалентные меры обеспечения ИБ (см. 14.3).

Дополнительная информация

Действия в ходе разработки и тестирования могут вызывать серьезные проблемы, например случайное изменение файлов, системной среды или системные сбои. Необходимо поддерживать понятную и стабильную среду, в которой можно проводить полноценное тестирование и предотвращать несанкционированный доступ разработчиков к среде эксплуатации.

Там, где персонал, занимающийся разработкой и тестированием, имеет доступ к среде эксплуатации и ее информации, он может иметь возможность внедрить неавторизованный и непроверенный код или изменить эксплуатационные данные. В некоторых системах эта возможность может использоваться для совершения мошенничества, внедрения непроверенного или вредоносного кода, что может вызвать серьезные проблемы в среде эксплуатации.

Персонал, занимающийся разработкой и тестированием, также представляет собой угрозу конфиденциальности эксплуатационной информации. Действия по разработке и тестированию могут привести к непреднамеренным изменениям программного обеспечения или информации, если они выполняются в одной вычислительной среде. Поэтому желательно разделять среду разработки, тестирования и эксплуатации, чтобы снизить риск случайного изменения или несанкционированного доступа к эксплуатируемому программного обеспечению и бизнес-данным (см. 14.3 о защите тестовых данных).

### 12.2 Защита от вредоносных программ

Цель: Обеспечить уверенность в защите информации и средств обработки информации от вредоносных программ.

#### 12.2.1 Меры обеспечения информационной безопасности в отношении вредоносных программ

Мера обеспечения ИБ

Для защиты от вредоносных программ должны быть реализованы меры обеспечения ИБ, связанные с обнаружением, предотвращением и восстановлением, в сочетании с соответствующим информированием пользователей.

Руководство по применению

Защита от вредоносных программ должна основываться на применении программного обеспечения для обнаружения вредоносных программ и восстановления данных, осведомленности об ИБ, соответствующих мерах контроля доступа к системе и управлению изменениями. Следует принять во внимание следующие рекомендации:

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

b) реализация мер обеспечения ИБ, которые предотвращают или обнаруживают использование неавторизованного программного обеспечения (например, белый список приложений);

c) внедрение мер обеспечения ИБ, которые предотвращают или обнаруживают обращение к известным или предполагаемым вредоносным веб-сайтам (например, ведение черного списка);

d) установление формальной политики для защиты от рисков, связанных с получением файлов и программного обеспечения из внешних сетей или через них, либо с помощью других способов, с указанием мер по защите;

e) снижение числа уязвимостей, которые могут быть использованы вредоносными программами, например через менеджмент технических уязвимостей (см. 12.6);

f) проведение регулярных проверок программного обеспечения и содержимого систем, поддерживающих критические бизнес-процессы; наличие любых несанкционированных файлов или неавторизованных изменений должно быть официально расследовано;

g) установка и регулярное обновление программного обеспечения для обнаружения вредоносных программ и восстановления, предназначенного для сканирования компьютеров и носителей в качестве предупреждающей меры или на регулярной основе; проводимое сканирование должно включать в себя:

1) проверку любых файлов, полученных по сети или через любой другой носитель, на наличие вредоносных программ перед использованием;

2) проверку вложений и загружаемых файлов электронной почты на наличие вредоносных программ перед использованием; такое сканирование должно проводиться в разных местах, например на серверах электронной почты, настольных компьютерах и на первой линии сети организации;

3) проверку веб-страницы на наличие вредоносных программ;

h) определение процедур и обязанностей по обеспечению защиты от вредоносных программ в системах, обучению их использованию, составлению отчетов и восстановлению после атак с применением вредоносных программ;

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

j) внедрение процедур регулярного сбора информации, таких как подписка на списки рассылки или посещение веб-сайтов, предоставляющих информацию о новых вредоносных программах;

k) внедрение процедур для проверки информации, относящейся к вредоносным программам, и обеспечения уверенности в том, что предупреждающие бюллетени точны и информативны; руководители должны гарантировать, что для дифференциации между реальными вредоносными программами и ложными используются квалифицированные источники, например авторитетные журналы, надежные веб-сайты или поставщики программного обеспечения по защите от вредоносных программ; все пользователи должны быть осведомлены о проблеме ложных вредоносных программ и о том, что необходимо делать при их получении;

l) изолирование сред, где могут возникнуть катастрофические последствия.

Дополнительная информация

Использование двух или более программных продуктов от разных поставщиков, которые основываются на различных технологиях защиты от вредоносных программ, в среде обработки информации может повысить эффективность защиты от вредоносных программ.

Следует проявлять осторожность при защите от внедрения вредоносного кода во время обслуживания и аварийных процедур, которые могут обойти обычные меры защиты от вредоносного программного обеспечения.

При определенных условиях защита от вредоносных программ может вызвать нарушения в работе средств обработки информации.

Использование в качестве меры защиты от вредоносного программного обеспечения только средства обнаружения и восстановления обычно недостаточно и требует сопровождения эксплуатационными процедурами для предотвращения внедрения вредоносных программ.

### 12.3 Резервное копирование

| |
|---|
| Цель: Обеспечить защиту от потери данных. |

#### 12.3.1 Резервное копирование информации

Мера обеспечения ИБ

В соответствии с политикой резервирования следует регулярно создавать и проверять резервные копии информации, программного обеспечения и образов системы.

Руководство по применению

Политика резервного копирования должна быть установлена для определения требований организации к резервному копированию информации, программного обеспечения и систем.

Политика резервного копирования должна определять требования к хранению и защите.

Должны быть предусмотрены надлежащие средства резервного копирования, чтобы обеспечить возможность восстановления всей важной информации и программного обеспечения после аварии или сбоя носителя.

При разработке плана резервного копирования следует принять во внимание следующее:

a) необходимо вести точный и полный учет резервных копий, а также документировать процедуры восстановления;

b) объем (например, полное или дифференциальное резервное копирование) и частота резервного копирования должны соответствовать бизнес-требованиям организации, требованиям безопасности, а также важности информации для непрерывной работы организации;

c) резервные копии должны храниться в удаленном месте на достаточном расстоянии, чтобы избежать какого-либо ущерба от аварии на основной площадке организации;

d) резервированная информация должна иметь соответствующий уровень защиты, как физической, так и от угроз окружающей среды (раздел 11) в соответствии со стандартами, применяемыми на основной площадке;

e) носители резервных копий следует регулярно проверять, чтобы гарантировать, что их можно использовать в случае экстренной необходимости; это должно совмещаться с проверкой процедур восстановления и затрачиваемого при этом времени. Тестирование возможности восстановления данных из резервной копии следует выполнять на выделенных для этого носителях, а не перезаписыванием информации на оригинальном носителе, поскольку в случае сбоя процесса резервного копирования или восстановления возможны необратимые повреждения или потеря данных;

f) в ситуациях, когда важна конфиденциальность, резервные копии следует защищать с помощью шифрования.

Эксплуатационные процедуры должны контролировать выполнение резервного копирования и обрабатывать сбои в ходе запланированного резервного копирования, чтобы обеспечить полноту и результативность резервного копирования в соответствии с политикой резервного копирования.

Для гарантии того, что механизмы резервного копирования соответствуют требованиям планов обеспечения непрерывности бизнеса, их следует регулярно проверять для каждой отдельной системы и службы. Для критических систем и служб механизмы резервного копирования должны охватывать всю системную информацию, приложения и данные, необходимые для восстановления всей системы в случае аварии.

Срок хранения информации, имеющей важное значение для бизнеса, должен быть определен с учетом всех требований к постоянному хранению архивных копий.

### 12.4 Регистрация и мониторинг

| |
|---|
| Цель: Регистрация событий безопасности и формирование свидетельств. |

#### 12.4.1 Регистрация событий

Мера обеспечения ИБ

Требуется обеспечивать формирование, ведение и регулярный анализ регистрационных журналов, фиксирующих действия пользователей, нештатные ситуации, ошибки и события безопасности.

Руководство по применению

Журналы событий, где это применимо, должны включать в себя:

a) пользовательские идентификаторы;

b) действия в системе;

c) дату, время и детали ключевых событий, например вход и выход из системы;

d) идентификатор устройства или местоположения, если возможно, и системный идентификатор;

e) записи об успешных и отклоненных попытках доступа к системе;

f) записи об успешных или отклоненных попытках доступа к данным и иным ресурсам;

g) изменения конфигурации системы;

h) использование привилегий;

i) использование системных служебных программ и приложений;

j) файлы, к которым был запрошен доступ, а также вид доступа;

k) сетевые адреса и протоколы;

l) сигналы тревоги от системы контроля управления доступом;

m) события активации и деактивации систем защиты, таких как антивирусные средства и системы обнаружения вторжений;

n) записи транзакций, выполненных пользователями в приложениях.

Ведение журнала событий служит основой для автоматизированных систем мониторинга, которые способны генерировать консолидированные отчеты и оповещения о безопасности системы.

Дополнительная информация

Журналы событий могут содержать информацию ограниченного доступа. Для обеспечения конфиденциальности должны быть приняты соответствующие меры защиты (см. 18.1.4).

Там, где это возможно, системные администраторы не должны иметь прав на удаление или деактивацию журналирования собственных действий (см. 12.4.3).

**12.4.2 Защита информации регистрационных журналов**

Мера обеспечения ИБ

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

Руководство по применению

Меры обеспечения ИБ должны быть направлены на защиту от несанкционированных изменений информации журнала и проблем, возникающих при эксплуатации средств регистрации, включая:

a) изменение типов сообщений, которые были записаны;

b) удаление или изменение журнала;

c) превышение емкости хранилища файлов журнала, что приводит к невозможности записи событий или перезаписи информации о прошлых событиях.

Может потребоваться сохранять в архиве некоторые журналы аудита как часть политики хранения записей или вследствие наличия требований по сбору и хранению доказательств (см. 16.1.7).

Дополнительная информация

Системные журналы часто содержат большой объем информации, большая часть которой не имеет отношения к мониторингу событий безопасности. Чтобы помочь идентифицировать важные с точки зрения мониторинга ИБ события, следует рассмотреть возможность автоматического копирования записей соответствующего типа во второй журнал, либо использовать подходящие системные служебные программы или инструменты аудита, которые позволят систематизировать файлы журналов.

Системные журналы должны быть защищены, так как, если данные в них можно изменить или удалить, то существование таких журналов может создать ложное чувство безопасности. Копирование журналов в реальном времени в систему, находящуюся вне контроля системного администратора или оператора, может применяться как мера обеспечения безопасности.

**12.4.3 Регистрационные журналы действий администратора и оператора**

Мера обеспечения ИБ

Действия системного администратора и оператора системы следует регистрировать, а регистрационные журналы защищать и регулярно анализировать.

Руководство по применению

Владельцы привилегированных учетных записей могут иметь возможность манипулировать журналами на средствах обработки информации, находящимися под их непосредственным управлением, следовательно, необходимо защищать и проверять журналы для обеспечения подотчетности привилегированных пользователей.

Дополнительная информация

Система обнаружения вторжений, находящаяся вне контроля системных и сетевых администраторов, может быть использована для мониторинга их действий на предмет соответствия.

**12.4.4 Синхронизация часов**

Мера обеспечения ИБ

Часы всех систем обработки информации в рамках организации или домена безопасности должны быть синхронизированы с единым эталонным источником времени.

Руководство по применению

Внешние и внутренние требования к представлению времени, синхронизаций и точности должны быть задокументированы. Такие требования могут быть правовыми, нормативными, договорными, являться требованиями стандартов или требованиями, касающимися внутреннего мониторинга. В организации должен быть определен стандартный эталон времени.

Подходы организации к получению эталонного времени из внешних источников и надежной синхронизации внутренних часов должны быть задокументированы и реализованы.

Дополнительная информация

Правильная настройка компьютерных часов важна для обеспечения точности журналов аудита, которые могут потребоваться для проведения расследований или в качестве доказательств в юридических или дисциплинарных спорах. Неточные журналы аудита могут препятствовать проведению таких расследований и подрывать достоверность таких доказательств. В качестве эталонного времени в системах регистрации могут быть использованы сигналы точного времени, передаваемые по радио и синхронизированные с национальными центрами стандартов времени и частоты. Для синхронизации всех серверов с эталоном может использоваться протокол сетевого времени (NTP).

### 12.5 Контроль программного обеспечения, находящегося в эксплуатации

Цель: Обеспечить уверенность в целостности систем, находящихся в эксплуатации.

#### 12.5.1 Установка программного обеспечения в эксплуатируемых системах

Мера обеспечения ИБ

Должны быть реализованы процедуры контроля установки программного обеспечения в системах, находящихся в эксплуатации.

Руководство по применению

Необходимо принять во внимание следующие рекомендации по управлению изменениями программного обеспечения в эксплуатируемых системах:

a) обновление эксплуатируемого программного обеспечения, приложений и программных библиотек должны выполнять только обученные администраторы при наличии соответствующего разрешения руководства (см. 9.4.5);

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

c) программное обеспечение и приложения следует внедрять в эксплуатируемую систему только после обширного и успешного тестирования; тесты должны охватывать удобство использования, безопасность, влияние на другие системы, дружелюбность интерфейса и должны проводиться на выделенных для этого системах (см. 12.1.4); следует убедиться, что все соответствующие исходные программные библиотеки были обновлены;

d) должна использоваться система управления конфигурацией для контроля над всем внедренным программным обеспечением и системной документацией;

e) перед внедрением изменений должна быть разработана стратегия возврата в исходное состояние;

f) следует вести журнал всех обновлений действующих программных библиотек;

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

h) старые версии программного обеспечения должны быть заархивированы вместе со всей необходимой информацией и параметрами, процедурами, деталями настройки и вспомогательным программным обеспечением на тот же срок, что и данные.

Поставляемое программное обеспечение, используемое в эксплуатируемых системах, должно поддерживаться на уровне, обеспечиваемом поставщиком. Со временем поставщики программного обеспечения перестанут поддерживать более старые версии программного обеспечения. Организация должна учитывать риски, связанные с использованием неподдерживаемого программного обеспечения.

Любое решение об обновлении до новой версии должно учитывать требования бизнеса по изменению и безопасности новой версии, например введение нового функционала, связанного с ИБ, или количество и серьезность проблем безопасности, связанных с этой версией. Пакеты исправлений программного обеспечения должны применяться тогда, когда они могут помочь устранить или снизить уязвимости ИБ (см. 12.6).

Физический или логический доступ должен предоставляться поставщикам только когда это необходимо для целей поддержки и с одобрения руководства. Действия поставщика следует контролировать (см. 15.2.1).

Компьютерное программное обеспечение может зависеть от поставляемого внешнего программного обеспечения и модулей, которые должны быть контролируемы и управляемы во избежание несанкционированных изменений, которые могут привести к уязвимостям в безопасности.

### 12.6 Менеджмент технических уязвимостей

| |
|---|
| Цель: Предотвратить использование технических уязвимостей. |

#### 12.6.1 Процесс управления техническими уязвимостями

Мера обеспечения ИБ

Должна быть своевременно получена информация о технических уязвимостях используемых информационных систем, оценена подверженность организации таким уязвимостям и приняты соответствующие меры в отношении связанного с этим риска ИБ.

Руководство по применению

Актуальный и полный перечень активов (раздел 8) является необходимым условием для эффективного управления техническими уязвимостями. Специальная информация, необходимая для поддержки управления техническими уязвимостями, включает в себя информацию о поставщике программного обеспечения, номерах версий, текущем состоянии развертывания (например, какое программное обеспечение установлено в каких системах) и работниках, ответственных за программное обеспечение в организации.

В ответ на выявление потенциальных технических уязвимостей должны быть предприняты надлежащие и своевременные действия. Необходимо придерживаться следующих указаний для создания эффективного процесса управления техническими уязвимостями:

a) организация должна определить и установить роли и обязанности, связанные с управлением техническими уязвимостями, включая их мониторинг, оценку риска, исправление ошибок, отслеживание активов и любые необходимые обязанности по координации процесса;

b) для программного обеспечения и других технологий (на основе перечня активов, см. 8.1.1) следует идентифицировать информационные ресурсы, которые будут использоваться для выявления соответствующих технических уязвимостей и поддержания осведомленности о них; эти информационные ресурсы должны обновляться в соответствии с изменениями в перечне активов или при обнаружении новых и полезных ресурсов;

c) следует определить сроки реагирования на уведомления о потенциально значимых технических уязвимостях;

d) после выявления потенциальной технической уязвимости организация должна определить связанные с ней риски и действия, которые необходимо предпринять; такие действия могут включать применение пакетов исправлений к уязвимым системам или применение компенсирующих мер обеспечения ИБ;

e) в зависимости от того, насколько срочно необходимо устранить техническую уязвимость, предпринимаемые действия должны проводиться в соответствии с мерами по управлению изменениями (см. 12.1.2) или в соответствии с процедурами реагирования на инциденты ИБ (см. 16.1.5);

f) если доступно официальное исправление, следует оценить риски, связанные с его установкой (риски, связанные с уязвимостью, следует сравнить с рисками, которые могут возникнуть вследствие установки исправления);

g) пакеты исправлений должны быть проверены и оценены до их установки, чтобы быть уверенным в том, что они не приведут к недопустимым побочным эффектам; если исправлений не выпущено, следует рассмотреть иные меры обеспечения информационной безопасности, такие как:

1) отключение сервисов и возможностей, связанных с уязвимостью;
2) настройка или добавление мер контроля доступа, например межсетевые экраны на границах сети (см. 13.1);
3) усиление мониторинга для выявления реальных атак;
4) повышение осведомленности об уязвимостях;

h) следует вести журнал всех предпринятых действий;

i) процесс управления техническими уязвимостями следует регулярно контролировать и оценивать для обеспечения его эффективности и результативности;

j) в первую очередь следует обращать внимание на системы с высоким уровнем риска;

k) эффективный процесс управления техническими уязвимостями должен быть согласован с действиями по управлению инцидентами, что позволит передавать данные об уязвимостях группе реагирования на инциденты и дополнит процесс техническими процедурами, которые должны быть выполнены в случае инцидента;

l) необходимо определить процедуру для решения ситуации, когда уязвимость была выявлена, но подходящих мер еще не существует. В этой ситуации организация должна оценить риски, связанные с известной уязвимостью, и определить соответствующие действия по обнаружению и корректировке.

Дополнительная информация

Управление техническими уязвимостями может рассматриваться как подфункция процесса управления изменениями и, как следствие, может использовать преимущества процессов и процедур управления изменениями (см. 12.1.2 и 14.2.2).

Производители часто испытывают на себе значительное давление, заключающееся в требовании выпускать пакеты исправлений как можно скорее. Следовательно существует вероятность того, что исправление не решает проблему должным образом и имеет отрицательные побочные эффекты. Кроме того, в некоторых случаях после применения исправления его удаление может оказаться проблематичным.

Если адекватное тестирование исправлений невозможно, например из-за затрат или нехватки ресурсов, то следует рассмотреть возможность задержки его применения и оценить связанные с этим риски, основываясь на опыте, полученном от других пользователей. Может оказаться полезным использование ИСО/МЭК 27031 [14].

**12.6.2 Ограничения на установку программного обеспечения**

Мера обеспечения ИБ

Должны быть установлены и реализованы правила, регулирующие установку программного обеспечения пользователями.

Руководство по применению

Организация должна определить и закрепить строгую политику в отношении того, какие типы программного обеспечения могут устанавливать пользователи.

Следует исходить из принципа наименьших привилегий. В случае предоставления определенных привилегий пользователи могут иметь возможность устанавливать программное обеспечение. Организация должна определить, какие виды установок разрешены (например, обновления и исправления безопасности для существующего программного обеспечения) и какие виды запрещены (например, программное обеспечение, предназначенное только для личного использования, и неизвестное программное обеспечение, которое потенциально может быть вредоносным). Эти привилегии должны предоставляться с учетом ролей соответствующих пользователей.

Дополнительная информация

Неконтролируемая установка программного обеспечения на вычислительные устройства может привести к появлению уязвимостей, а затем к утечке информации, нарушению целостности или другим инцидентами ИБ, либо к нарушению прав на интеллектуальную собственность.

### 12.7 Особенности аудита информационных систем

Цель: Минимизировать влияние аудиторской деятельности на функционирование систем, находящихся в эксплуатации.

**12.7.1 Меры обеспечения информационной безопасности в отношении аудита информационных систем**

Мера обеспечения ИБ

Требования к процессу регистрации событий [аудиту] и деятельности, связанной с контролем находящихся в эксплуатации систем, должны быть тщательно спланированы и согласованы для минимизации сбоев в бизнес-процессах.

Руководство по применению

Необходимо придерживаться следующих рекомендаций:

a) требования доступа к системам и данным для проведения аудита должны быть согласованы с соответствующим руководством;

b) область действия технического аудита должна быть согласована и проконтролирована;

c) аудиторские тесты должны быть ограничены доступом уровня «только на чтение» в отношении программного обеспечения и данных;

d) доступ, отличный от режима «только на чтение», должен быть разрешен только для изолированных копий системных файлов, которые должны быть уничтожены по завершении аудита или обеспечены соответствующей защитой, если существует необходимость сохранять такие файлы в соответствии с требованиями документации по аудиту;

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

f) аудиторские тесты, которые могут повлиять на доступность системы, следует проводить в нерабочее время;

g) любой доступ должен контролироваться и регистрироваться для создания прослеживаемости.

## 13 Безопасность коммуникаций

### 13.1 Менеджмент информационной безопасности сетей

Цель: Обеспечить защиту информации в сетях и в образующих их средствах обработки информации.

#### 13.1.1 Меры обеспечения информационной безопасности сетей

Мера обеспечения ИБ

Сети должны управляться и контролироваться для обеспечения защиты информации в системах и приложениях.

Руководство по применению

Должны быть реализованы меры для обеспечения безопасности информации в сетях и защиты подключенных сервисов от несанкционированного доступа. В частности, следует учитывать следующее:

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

b) там, где это применимо, обязанности по эксплуатации сетей должны быть отделены от обязанностей по эксплуатации компьютеров (см. 6.1.2);

c) должны быть установлены специальные меры обеспечения ИБ для защиты конфиденциальности и целостности данных, передаваемых по сетям общего пользования или беспроводным сетям, и для защиты подключенных систем и приложений (раздел 10 и 13.2); могут потребоваться специальные меры для обеспечения доступности сетевых сервисов и подключенных компьютеров;

d) должна вестись соответствующая регистрация и мониторинг с целью фиксации и обнаружения действий, которые могут повлиять на ИБ или имеют отношение к ней;

e) действия по управлению должны быть тесно координированы как для того, чтобы оптимизировать обслуживание организации, так и для обеспечения того, чтобы меры обеспечения безопасности применялись согласованно в рамках всей инфраструктуры обработки информации;

f) системы в сетях должны проходить процедуру аутентификации;

g) подключение систем к сети должно быть ограничено.

Дополнительная информация

Дополнительную информацию о сетевой безопасности можно найти в ИСО/МЭК 27033 [15], [16], [17], [18], [19].

#### 13.1.2 Безопасность сетевых сервисов

Мера обеспечения ИБ

Механизмы обеспечения безопасности, уровни обслуживания и требования к управлению для всех сетевых сервисов должны быть идентифицированы и включены в соглашения по сетевым сервисам независимо от того, будут ли они обеспечиваться силами организации или осуществляться с использованием аутсорсинга.

Руководство по применению

Следует определить и регулярно подвергать мониторингу способность поставщика сетевых сервисов безопасно управлять сервисами, определенными договором, а право проведения аудита должно быть согласовано.

Должны быть определены меры по обеспечению безопасности, необходимые для конкретных сервисов, такие как функции безопасности, уровни обслуживания и требования к управлению. Организация должна гарантировать, что поставщики сетевых сервисов реализуют эти меры.

Дополнительная информация

Сетевые сервисы включают в себя обеспечение соединений, сервисы частных сетей и сетей с расширенными возможностями, а также решения, касающиеся управления безопасностью сети, такие как межсетевые экраны и системы обнаружения вторжений. Эти сервисы могут варьироваться в диа-

пазоне от простого предоставления неуправляемой полосы пропускания до сложных решений с дополнительными услугами.

Функциями безопасности сетевых сервисов могут быть:

a) технологии, применяемые для обеспечения безопасности сетевых сервисов, например аутентификация, шифрование и контроль сетевых подключений;

b) технические параметры, необходимые для безопасного подключения к сетевым сервисам в соответствии с правилами безопасности сетевых соединений;

c) процедуры использования сетевых сервисов, применяемые с целью ограничения доступа к сетевым сервисам или приложениям, где это необходимо.

**13.1.3 Разделение в сетях**

Мера обеспечения ИБ

Группы информационных сервисов, пользователей и информационных систем в сети должны быть разделены.

Руководство по применению

Одним из методов управления безопасностью больших сетей является разделение их на отдельные сетевые домены. Домены могут быть выбраны на основе уровней доверия (например, общедоступный домен, домен рабочих станций, домен сервера), на основе организационных подразделений (например, кадры, финансы, маркетинг) или на основе некоторой комбинации признаков (например, домен сервера, соединенный с несколькими организационными подразделениями). Разделение может быть выполнено физическим разделением на разные сети либо логическим (например, виртуальные частные сети).

Границы каждого домена должны быть четко определены. Доступ между сетевыми доменами может быть разрешен, но должен контролироваться на границе с использованием шлюза (например, межсетевого экрана, фильтрующего маршрутизатора). Критерии разделения сетей на домены и разрешение доступа через шлюзы должны основываться на оценке требований по безопасности каждого домена. Оценка должна проводиться в соответствии с политикой управления доступом (см. 9.1.1) и требованиями к доступу, в соответствии с ценностью и категорией обрабатываемой информации, а также с учетом относительной стоимости и влияния применяемой технологии шлюза на производительность.

Беспроводные сети требуют особого подхода в силу того, что их границы не являются достаточно определенными. В отношении чувствительных сегментов следует принять подход, при котором все запросы на беспроводной доступ следует рассматривать как внешние и отделять их от запросов внутренних сетей до тех пор, пока запрос не пройдет шлюз и не будет разрешен доступ к внутренним системам в соответствии с политикой обеспечения ИБ сетей (см. 13.1.1).

Технологии аутентификации, шифрования и управления доступом к сети на уровне пользователя, основанные на современных стандартах беспроводных сетей, при должной реализации могут быть достаточными для прямого подключения к внутренней сети организации.

Дополнительная информация

Сети часто выходят за границы организации, поскольку создаются деловые отношения, которые требуют объединения или совместного использования сетевого оборудования и устройств обработки информации. Такие действия могут увеличивать риск неавторизованного доступа к информационным системам организации, использующим сеть, причем в отношении некоторых из этих систем может потребоваться защита от пользователей другой сети в силу их чувствительности или критичности.

### 13.2 Передача информации

Цель: Поддерживать безопасность информации, передаваемой как внутри организации, так и при обмене с любым внешним объектом и субъектом.

**13.2.1 Политики и процедуры передачи информации**

Мера обеспечения ИБ

Должны существовать формализованные политики и процедуры передачи информации, а также соответствующие меры, обеспечивающие безопасность информации, передаваемой с использованием всех видов средств связи.

Руководство по применению

Процедуры и меры обеспечения ИБ, которым необходимо следовать при использовании средств связи для передачи информации, должны учитывать следующее:

a) процедуры, предназначенные для защиты передаваемой информации от перехвата, копирования, модификации, перенаправления и уничтожения;

b) процедуры обнаружения и защиты от вредоносных программ, которые могут передаваться с использованием электронных средств связи (см. 12.2.1);

c) процедуры для защиты информации ограниченного доступа в электронном виде, передаваемой в форме вложения;

d) политику или руководства, определяющие допустимое использование средств связи (см. 8.1.3);

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

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

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

h) меры обеспечения ИБ и ограничения, связанные с использованием средств связи, например автоматическая пересылка электронной почты на внешние почтовые адреса;

i) рекомендации персоналу предпринимать меры предосторожности во избежание раскрытия конфиденциальной информации;

j) не оставлять сообщения, содержащие конфиденциальную информацию на автоответчиках, так как они могут быть прослушаны неавторизованными лицами, сохранены в системах общего пользования или некорректно записаны в результате ошибочного набора номера;

k) консультирование персонала о проблемах, связанных с использованием факсов и соответствующих услуг, а именно:

1) неавторизованный доступ к встроенным хранилищам сообщений для извлечения сообщений;

2) преднамеренное или случайное программирование машин на отправку сообщений на определенные номера;

3) отсылка документов и сообщений на неверный номер в результате ошибочного набора либо вызова сохраненного неверного номера.

Кроме того, персоналу следует напоминать, что не следует вести конфиденциальные разговоры в общественных местах или по небезопасным каналам связи, в открытых офисах и переговорных.

Услуги по передаче информации должны соответствовать всем релевантным требованиям законодательства (см. 18.1).

Дополнительная информация

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

Передача программного обеспечения может осуществляться различными способами, включая загрузку из Интернета и приобретение у поставщиков, продающих готовые продукты.

Следует учитывать юридические последствия, влияние на бизнес и безопасность, связанные с обменом электронными данными, электронной торговлей и электронной связью, а также требования к мерам обеспечения ИБ.

**13.2.2 Соглашения о передаче информации**

Мера обеспечения ИБ

Безопасная передача деловой информации между организацией и внешними сторонами должна быть определена соглашениями.

Руководство по применению

Соглашения по передаче информации должны включать в себя следующее:

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

b) процедуры для обеспечения прослеживаемости и неотказуемости;

c) минимальные требования технических стандартов для упаковки и передачи;

d) соглашения условного депонирования (эскроу);

e) стандарты по идентификации курьеров;

f) ответственность и обязательства в случае инцидентов ИБ, таких как потеря данных;

g) использование согласованной системы маркирования для информации ограниченного доступа, гарантирующей, что значение этой маркировки будет сразу же понято и что информация будет соответствующим образом защищена (см. 8.2);

h) технические стандарты для записи и чтения информации и программного обеспечения;

i) любые специальные меры обеспечения ИБ, которые требуются для защиты чувствительных элементов, например криптография (раздел 10);

j) поддержание цепочки сохранности информации в процессе передачи;

k) приемлемые уровни управления доступом.

Должны быть разработаны и поддерживаться политики, процедуры и стандарты по защите информации и физических носителей в процессе передачи (см. 8.3.3), на них следует ссылаться в соглашениях о передаче.

Часть любого соглашения, посвященного ИБ, должна отражать степень доступности деловой информации.

Дополнительная информация

Соглашения могут быть в электронном или бумажном виде и могут иметь форму официальных договоров. Конкретные механизмы, используемые для передачи конфиденциальной информации, должны быть согласованы для всех организаций и типов соглашений.

**13.2.3 Электронный обмен сообщениями**

Мера обеспечения ИБ

Следует обеспечивать соответствующую защиту информации при электронном обмене сообщениями.

Руководство по применению

Соображения по обеспечению ИБ электронных сообщений должны включать следующее:

a) защиту сообщений от несанкционированного доступа, изменения или отказа в обслуживании в соответствии с системой категорирования, принятой в организации;

b) обеспечение правильной адресации и передачи сообщения;

c) надежность и доступность сервиса;

d) правовые аспекты, например требования к электронным подписям;

e) получение одобрения до использования внешних общедоступных сервисов, например сервисов мгновенных сообщений, социальных сетей или сервисов обмена файлами;

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

Дополнительная информация

Существует много типов электронных сообщений, таких как электронная почта, обмен электронными данными и социальные сети, которые играют важную роль в деловых отношениях.

**13.2.4 Соглашения о конфиденциальности или неразглашении**

Мера обеспечения ИБ

Требования в отношении соглашений о конфиденциальности или неразглашении, отражающие потребности организации в обеспечении защиты информации, должны быть идентифицированы, документально оформлены и регулярно пересматриваться.

Руководство по применению

В соглашениях о конфиденциальности или неразглашении должно содержаться требование по защите конфиденциальной информации, выраженное юридическими терминами, имеющими исковую силу. Соглашения о конфиденциальности или неразглашении применимы к внешним сторонам или работникам организации. Содержание соглашения должно определяться с учетом типа другой стороны, предоставляемого доступа или обработки конфиденциальной информации. При определении требований к соглашениям о конфиденциальности или неразглашении необходимо учитывать следующее:

a) определение информации, подлежащей защите (например, конфиденциальной информации);

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

c) действия, необходимые при расторжении соглашения;

d) обязанности и действия лиц, подписавших соглашение, во избежание несанкционированного раскрытия информации;

e) право собственности на информацию, коммерческую тайну и интеллектуальную собственность и то, как это связано с защитой конфиденциальной информации;

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

g) право на аудит и мониторинг деятельности, связанной с конфиденциальной информацией;

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

i) условия, при которых информация должна быть возвращена или уничтожена в случае прекращения действия соглашения;

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

Исходя из требований ИБ организации, может потребоваться добавление других элементов в соглашения о конфиденциальности или неразглашении.

Соглашения о конфиденциальности и неразглашении должны соответствовать всем применимым законам и нормативным документам, под юрисдикцию которых они подпадают (см. 18.1).

Требования соглашений о конфиденциальности и неразглашении следует пересматривать периодически и в тех случаях, когда происходят изменения, затрагивающие эти требования.

Дополнительная информация

Соглашения о конфиденциальности и неразглашении защищают информацию организации, а также надежным и правомочным образом информируют лиц, подписавших соглашение, об их ответственности за защиту, использование и разглашение информации.

В зависимости от различных обстоятельств организации могут потребоваться различные формы соглашений о конфиденциальности или неразглашении.

## 14 Приобретение, разработка и поддержка систем

### 14.1 Требования к безопасности информационных систем

Цель: Обеспечить уверенность в том, что ИБ является неотъемлемой частью информационных систем на протяжении всего их жизненного цикла и включает требования к информационным системам, предоставляющим услуги с использованием сетей общего пользования.

#### 14.1.1 Анализ и спецификация требований информационной безопасности

Мера обеспечения ИБ

Требования, относящиеся к ИБ, должны быть включены в перечень требований для новых информационных систем или для усовершенствования существующих информационных систем.

Руководство по применению

Требования ИБ должны быть идентифицированы с использованием различных методов, таких как выделение требований соответствия из политик и регламентов, моделирование угроз, анализ инцидентов или использование порогов уязвимости. Результаты идентификации должны быть задокументированы и рассмотрены всеми заинтересованными сторонами.

Требования и меры обеспечения ИБ должны отражать ценность информации (см. 8.2) и потенциальное негативное влияние на бизнес, которое может быть вызвано отсутствием надлежащей защиты.

Идентификация и управление требованиями ИБ и связанными с этими процессами должны быть интегрированы в проекты информационных систем на ранних стадиях. Раннее рассмотрение требований ИБ, например на этапе проектирования, может дать более эффективные и менее затратные решения.

Требования ИБ также должны учитывать:

a) требуемый уровень доверия в отношении идентификационной информации пользователей для установления требований к аутентификации пользователей;

b) процессы предоставления доступа как для пользователей, так и для привилегированных или технических пользователей;

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

d) необходимый уровень защиты в отношении затронутых активов, в частности в отношении доступности, конфиденциальности и целостности;

e) требования, вытекающие из бизнес-процессов, такие как ведение журнала и мониторинг транзакций, требования по обеспечению неотказуемости;

f) требования, предписанные другими мерами обеспечения ИБ, например интерфейсы для систем регистрации, мониторинга или обнаружения утечки данных.

Для приложений, которые предоставляют услуги через общедоступные сети или осуществляют транзакции, следует рассмотреть меры обеспечения ИБ, которые приведены в 14.1.2 и 14.1.3.

В случае приобретения продукта следует придерживаться формального процесса тестирования и приобретения. В договорах с поставщиком должны быть учтены установленные требования безопасности. Если функциональные возможности обеспечения безопасности в предлагаемом продукте не удовлетворяют указанным требованиям, порождаемый этим риск и связанные с ним меры должны быть рассмотрены до того, как продукт будет приобретен.

Имеющееся руководство по настройке мер обеспечения безопасности продукта, соответствующее финальному стеку программного обеспечения/сервисов системы, должно быть оценено и выполнено.

Должны быть определены критерии приемки продуктов, например с точки зрения их функциональности, что даст гарантию того, что установленные требования безопасности будут выполнены. Продукты должны быть оценены по этим критериям до их приобретения. Дополнительный функционал продукта также должен быть рассмотрен, чтобы убедиться, что он не порождает дополнительных неприемлемых рисков.

Дополнительная информация

ИСО/МЭК 27005 [11] и ИСО 31000 [27] предоставляют руководство по применению процессов управления рисками для идентификации мер обеспечения ИБ и выполнения требований.

**14.1.2 Обеспечение безопасности прикладных сервисов, предоставляемых с использованием сетей общего пользования**

Мера обеспечения ИБ

Информация, используемая в прикладных сервисах и передаваемая по сетям общего пользования, должна быть защищена от мошеннической деятельности, оспаривания договоров, а также несанкционированного раскрытия и модификации.

Руководство по применению

ИБ прикладных сервисов, проходящих через общедоступные сети, следует обеспечивать исходя из следующих соображений:

a) уровень доверия, который требует каждая сторона в отношении друг друга, например посредством аутентификации;

b) процессы авторизации, связанные с тем, кто может утверждать содержание, выпускать или подписывать ключевые деловые документы;

c) обеспечение того, чтобы взаимодействующие стороны были полностью проинформированы о своих правах на предоставление и использование сервиса;

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

e) уровень доверия, необходимый для целостности ключевых документов;

f) требования по защите любой конфиденциальной информации;

g) конфиденциальность и целостность любых операций с заказом, платежной информации, адреса доставки и подтверждения получения;

h) степень проверки платежной информации, предоставленной клиентом;

i) выбор наиболее подходящей формы расчета для защиты от мошенничества;

j) уровень защиты, необходимый для сохранения конфиденциальности и целостности информации о заказе;

k) предотвращение потери или дублирования информации об операции;

l) ответственность за мошеннические операции;

m) страховые требования.

Многие из вышеперечисленных соображений могут быть выполнены с применением криптографических мер обеспечения ИБ (раздел 10), принимая во внимание требования законодательства (раздел 18, особенно 18.1.5 для законодательства о криптографии).

Механизмы предоставления услуг между участниками должны быть закреплены документально оформленным соглашением, в котором обе стороны соглашаются с условиями предоставления сервисов, включая детали авторизации (перечисление b).

Следует учитывать требования устойчивости к атакам, которые могут включать в себя требования по защите используемых серверов приложений или обеспечению доступности сетевых соединений, необходимых для предоставления сервиса.

Дополнительная информация

Приложения, доступные через сети общего пользования, подвержены целому ряду угроз, таких как мошеннические действия, нарушение условий договора или публичное разглашение информации. Поэтому обязательным здесь является детальная оценка риска и правильный выбор мер обеспечения ИБ. Необходимые меры обеспечения ИБ часто включают в себя криптографические методы для аутентификации и защиты данных при передаче.

Прикладные сервисы могут использовать безопасные методы аутентификации, например использование криптографии с открытым ключом и электронных подписей (раздел 10) для снижения рисков. Кроме того, при необходимости, могут быть задействованы доверенные третьи стороны.

**14.1.3 Защита транзакций прикладных сервисов**

Мера обеспечения ИБ

Информацию, используемую в транзакциях прикладных сервисов, следует защищать для предотвращения неполной передачи, ложной маршрутизации, несанкционированного изменения, раскрытия, дублирования или воспроизведения сообщений.

Руководство по применению

Вопросы безопасности для транзакций прикладных сервисов должны включать следующее:

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

b) все аспекты транзакции, то есть обеспечение того, что:

1) секретная аутентификационная информация пользователей с каждой стороны проверена и действительна;

2) транзакция остается конфиденциальной;

3) сохраняется конфиденциальность всех вовлеченных сторон;

c) канал связи между всеми вовлеченными сторонами защищен;

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

e) обеспечение того, чтобы хранение деталей транзакции находилось за пределами какой-либо общедоступной среды, например в хранилище интрасети организации, которое не доступно непосредственно из сети Интернет;

f) если используется доверенный орган (например, для целей выдачи и поддержки электронных подписей или цифровых сертификатов), обеспечение безопасности интегрируется и становится частью процесса управления сертификатами/подписями на протяжении всего жизненного цикла такого процесса.

Дополнительная информация

Объем принятых мер обеспечения ИБ должен соответствовать уровню риска, связанного с каждой формой транзакции прикладных сервисов.

Транзакции должны соответствовать юридическим и нормативным требованиям той юрисдикции, где их формируют, обрабатывают, завершают или хранят.

### 14.2 Безопасность в процессах разработки и поддержки

Цель: Обеспечить уверенность в том, что меры обеспечения ИБ спроектированы и внедрены на всех стадиях жизненного цикла разработки информационных систем.

**14.2.1 Политика безопасной разработки**

Мера обеспечения ИБ

Правила разработки программного обеспечения и систем должны быть установлены и применены к разработкам в рамках организации.

Руководство по применению

Безопасная разработка — это требование для создания безопасного сервиса, архитектуры, программного обеспечения и системы. В рамках политики безопасной разработки должны быть учтены следующие аспекты:

a) безопасность среды разработки;

b) руководство по безопасности в жизненном цикле разработки программного обеспечения:

1) безопасность в методологии разработки программного обеспечения;

2) правила по безопасному программированию для каждого используемого языка программирования;

c) требования безопасности на этапе проектирования;

d) контрольные точки по проверке безопасности в рамках основных этапов проекта;

e) безопасные репозитории;

f) безопасность в управлении версиями;

g) необходимые знания по безопасности приложений;

h) способность разработчиков избегать, находить и исправлять уязвимости.

Методы безопасного программирования должны применяться как в отношении новых разработок, так и в случае повторного использования кода, при разработке которого использованы неизвестные стандарты или использованные стандарты не соответствуют лучшим практикам. Следует рассмотреть и, в случае необходимости, сделать обязательными для применения стандарты безопасного программирования. Разработчики должны быть обучены применению этих стандартов и тестированию, а анализ кода должен служить проверкой их использования.

Если разработка осуществляется на аутсорсинге, организация должна получить гарантии того, что внешняя сторона соблюдает правила по безопасной разработке (см. 14.2.7).

Дополнительная информация

Разработка также может вестись внутри самих приложений, например в офисных приложениях, скриптах, браузерах и базах данных.

**14.2.2 Процедуры управления изменениями системы**

Мера обеспечения ИБ

Необходимо управлять изменениями в системах в течение жизненного цикла разработки посредством применения формализованных процедур управления изменениями.

Руководство по применению

Формальные процедуры управления изменениями должны быть задокументированы и применены для обеспечения целостности системы, приложений и продуктов, начиная с ранних этапов проектирования и до всех последующих действий по поддержке. Внедрение новых систем и значительные изменения в существующих системах должны происходить в соответствии с формальным процессом документирования, спецификации, тестирования, контроля качества и управляемой реализации.

Этот процесс должен включать оценку риска, анализ последствий от изменений и определение необходимых мер обеспечения ИБ, а также должен гарантировать, что существующие меры не будут нарушены, что программистам поддержки предоставлен доступ только к тем частям системы, которые необходимы для их работы, и что получено формальное согласие на любые изменения и их одобрение.

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

a) ведение учета согласованных уровней разрешений;

b) обеспечение внесения изменений авторизованными пользователями;

c) пересмотр процедур управления и целостности для гарантии того, что они не будут нарушены изменениями;

d) идентификация всего программного обеспечения, информации, объектов базы данных и аппаратного обеспечения, которые требуют изменений;

e) выявление и проверка критического с точки зрения безопасности кода для минимизации вероятности реализации известных ошибок программирования;

f) получение официального одобрения на предлагаемые изменения до начала работ;

g) обеспечение того, чтобы авторизованные пользователи одобрили все изменения до их реализации;

h) обеспечение того, чтобы набор системной документации был обновлен по завершении каждого изменения, а старая документация архивировалась или удалялась;

i) поддержание контроля версий всех обновлений программного обеспечения;

j) ведение записей всех запросов на изменение;

k) обеспечение того, чтобы эксплуатационная документация (см. 12.1.1) и пользовательские процедуры подвергались изменениям по мере необходимости и оставались актуальными;

l) обеспечение того, чтобы внедрение изменений происходило в согласованное время и не нарушало вовлеченные бизнес-процессы.

Дополнительная информация

Так же как изменение программного обеспечения может повлиять на среду эксплуатации, так и наоборот.

Общепринятая практика включает в себя тестирование нового программного обеспечения в среде, отделенной как от среды эксплуатации, так и от среды разработки (см. 12.1.4). Это позволит иметь средства управления над новым программным обеспечением и обеспечивает дополнительную защиту эксплуатационной информации, которая используется в целях тестирования. Это относится к пакетам обновлений и исправлений, а также к прочим типам обновлений.

В тех случаях, где рассматривается автоматическое применение обновлений, риск в отношении целостности и доступности системы должен быть сопоставлен с преимуществами быстрого развертывания обновлений. Автоматические обновления не должны использоваться в критических системах, так как некоторые из них могут привести к сбою критических приложений.

**14.2.3 Техническая экспертиза приложений (прикладных программ) после изменений операционной платформы**

Мера обеспечения ИБ

При внесении изменений в операционные платформы критически важные для бизнеса приложения должны быть проверены и протестированы, чтобы обеспечить уверенность в отсутствии неблагоприятного воздействия на деятельность или безопасность организации.

Руководство по применению

Этот процесс должен охватывать:

a) пересмотр мер защиты приложения и процедур целостности для гарантии того, что они не будут нарушены изменениями в эксплуатируемой среде;

b) обеспечение своевременного уведомления об изменениях эксплуатируемой платформы с учетом времени проведения соответствующих тестов и проверки перед внедрением;

c) обеспечение внесения соответствующих изменений в планы обеспечения непрерывности бизнеса (раздел 17).

Дополнительная информация

Эксплуатируемые платформы включают в себя операционные системы, базы данных и связующее программное обеспечение. Меры обеспечения ИБ также должны применяться для процесса изменения приложений.

**14.2.4 Ограничения на изменения пакетов программ**

Мера обеспечения ИБ

Следует избегать модификаций пакетов программ, ограничиваться необходимыми изменениями и строго контролировать все изменения.

Руководство по применению

Насколько это возможно и практически осуществимо, пакеты программного обеспечения, приобретаемые у поставщика, следует использовать без изменений. Если требуется модифицировать пакет программ, необходимо учитывать следующее:

a) возможен риск нарушения встроенных средств контроля целостности;

b) должно ли быть получено согласие поставщика;

c) возможность получения необходимых изменений от поставщика в виде стандартных обновлений программы;

d) возможные последствия в случае, если организация станет ответственной за последующее сопровождение программного обеспечения в результате внесенных изменений;

e) совместимость с другим используемым программным обеспечением.

При необходимости внесения изменений оригинальное программное обеспечение должно быть сохранено, а изменения должны применяться к четко определенной копии. Процесс управления обновлениями программного обеспечения должен быть реализован для обеспечения того, чтобы для всего разрешенного программного обеспечения устанавливались самые последние утвержденные исправления и обновления (см. 2.6.1). Все изменения должны быть полностью протестированы и задокументированы, чтобы при необходимости их можно было применить к будущим обновлениям программного обеспечения. При необходимости изменения должны быть проверены и подтверждены независимым органом по оценке.

**14.2.5 Принципы безопасного проектирования систем**

Мера обеспечения ИБ

Принципы безопасного проектирования систем должны быть установлены, задокументированы, поддерживаться и применяться к любым работам по реализации информационной системы.

Руководство по применению

Процедуры безопасного проектирования информационных систем, основанные на указанных выше принципах, должны быть установлены, задокументированы и применены к внутренним процессам по проектированию информационных систем. Безопасность должна проектироваться на всех уровнях архитектуры (бизнес, данные, приложения и технологии), чтобы сбалансировать потребность в ИБ и удобстве. Новые технологии должны быть проанализированы на предмет угроз безопасности, а решения должны быть рассмотрены с точки зрения известных шаблонов атак.

Эти принципы и установленные процедуры проектирования должны регулярно пересматриваться, чтобы гарантировать, что они эффективно способствуют развитию стандартов безопасности в процессе проектирования. Их также следует регулярно пересматривать, чтобы обеспечить их актуальность с точки зрения борьбы с любыми потенциальными новыми угрозами и их пригодности к постоянно улучшающимся применяемым технологиям и решениям.

Установленные принципы безопасного проектирования должны применяться, по возможности, к информационным системам, находящимся на аутсорсинге, при помощи обязательных соглашений и контрактов между организацией и поставщиком. Организация должна подтвердить, что строгость принципов безопасного проектирования сопоставима с ее собственными.

Дополнительная информация

Процедуры разработки приложений должны применять методы безопасного проектирования при разработке приложений, имеющих интерфейсы ввода и вывода. Методы безопасного проектирования предоставляют методическую основу для методов аутентификации пользователей, безопасного управления сессиями и валидации данных, санитизации и удаления отладочной информации.

**14.2.6 Безопасная среда разработки**

Мера обеспечения ИБ

Организация должна установить и надлежащим образом защищать безопасные среды разработки, используемые для разработки и интеграции систем на всех стадиях жизненного цикла разработки системы.

Руководство по применению

Безопасная среда разработки включает в себя людей, процессы и технологии, связанные с разработкой и интеграцией систем.

Организации должны оценивать риски, связанные с определенными действиями по разработке систем, и формировать безопасные среды разработки для конкретных работ по разработке систем, учитывая:

a) информацию ограниченного доступа, подлежащую обработке, хранению и передаче системой;
b) применимые внешние и внутренние требования, например из нормативных актов или политик;
c) меры обеспечения ИБ, уже внедренные организацией для обеспечения разработки систем;
d) надежность персонала, работающего в среде (см. 7.1.1);
e) степень аутсорсинга работ, связанных с разработкой систем;
f) необходимость разделения различных сред разработки;
g) меры разграничения доступа к среде разработки;
h) мониторинг изменений среды и хранимого в ней кода;
i) резервные копии хранятся в безопасных удаленных местах;
j) контроль за перемещением данных из и в среду разработки.

Как только для конкретной среды разработки определен уровень защиты, организация должна задокументировать соответствующие процессы в процедурах безопасной разработки и довести их до сведения всех лиц, которые в них нуждаются.

**14.2.7 Разработка с использованием аутсорсинга**

Мера обеспечения ИБ

Организация должна осуществлять надзор за разработкой систем, выполняемой подрядчиками, и ее мониторинг.

Руководство по применению

В тех случаях, когда разработка системы осуществляется сторонними организациями, для всей цепочки поставок организации необходимо учесть следующее:

a) лицензионные соглашения, права на код и интеллектуальную собственность, связанные с находящимися на аутсорсинге разработками (см. 18.1.2);

b) договорные требования к безопасным методам проектирования, программирования и тестирования (см. 14.2.1);

c) предоставление утвержденной модели угроз внешнему разработчику;

d) приемочные испытания на качество и точность результатов;

e) предоставление доказательств того, что были применены пороговые критерии безопасности для установления минимально приемлемых уровней защищенности и конфиденциальности;

f) предоставление доказательств того, что было выполнено тестирование в достаточном объеме, чтобы подтвердить отсутствие преднамеренного или непреднамеренного вредоносного содержимого в поставляемых продуктах;

g) предоставление доказательств того, что было проведено достаточное тестирование для защиты от известных уязвимостей;

h) механизмы условного депонирования, например, если исходный код больше недоступен;

i) закрепленное в договоре право на аудит процессов и мер разработки;

j) действующая документация среды сборки, используемая для создания конечных продуктов;

k) организация несет ответственность за соблюдение действующего законодательства и проверку эффективности мер обеспечения ИБ.

Дополнительная информация

Дополнительную информацию об отношениях с поставщиками можно найти в ИСО/МЭК 27036 [21], [22], [23].

**14.2.8 Тестирование безопасности систем**

Мера обеспечения ИБ

Тестирование функциональных возможностей безопасности должно осуществляться в процессе разработки.

Руководство по применению

Новые и обновляемые системы требуют тщательного тестирования и проверки в ходе процесса разработки, включая подготовку подробного графика работ, а также входных данных и ожидаемых результатов при различных условиях тестирования. Для собственных разработок такие тесты должны первоначально выполняться командой разработки. Затем должно быть проведено независимое приемочное тестирование (как для внутренних, так и для находящихся на аутсорсинге разработок), чтобы убедиться, что система работает только так, как и ожидается (см. 14.1.1, 14.2.9). Глубина тестирования должна быть пропорциональна важности и характеру системы. (Внесена техническая поправка Cor.2:2015).

**14.2.9 Приемо-сдаточные испытания системы**

Мера обеспечения ИБ

Для новых информационных систем, обновлений и новых версий должны быть разработаны программы приемо-сдаточных испытаний и установлены связанные с ними критерии.

Руководство по применению

Приемочные испытания должны включать в себя проверку выполнения требований по ИБ (см. 14.1.1, 14.1.2) и соблюдение правил безопасной разработки системы (см. 14.2.1). Тестирование также должно проводиться в отношении заимствованных компонентов и интегрированных систем. Организации могут использовать автоматизированные инструменты, такие как анализаторы кода или сканеры уязвимостей, и должны гарантировать исправление связанных с безопасностью дефектов.

Испытания следует проводить в реалистичной среде тестирования, чтобы гарантировать надежность результатов и невозможность создания системой дополнительных уязвимостей в среде организации.

**14.3 Тестовые данные**

Цель: Обеспечить защиту данных, используемых для тестирования.

**14.3.1 Защита тестовых данных**

Мера обеспечения ИБ

Тестовые данные следует тщательно выбирать, защищать и контролировать.

Руководство по применению

Следует избегать использования данных из эксплуатируемой среды, содержащих персональные данные или любую другую конфиденциальную информацию, в целях тестирования. Если для целей тестирования используется такая информация, все конфиденциальные данные и содержимое должно быть защищено путем удаления или модификации (см. ИСО/МЭК 29101 [26]).

Для защиты эксплуатационных данных, используемых в целях тестирования, должны применяться следующие рекомендации:

a) процедуры контроля доступа, которые применяются к эксплуатируемым прикладным системам, должны также применяться к тестовым прикладным системам;

b) необходимо запрашивать разрешение каждый раз, когда эксплуатируемые данные копируются в тестовую среду;

c) информация из эксплуатируемой среды должна быть удалена из тестовой среды сразу после завершения тестирования;

d) копирование и использование информации из эксплуатируемой среды должно регистрироваться для обеспечения аудита.

Дополнительная информация

Системные и приемочные испытания обычно требуют значительных объемов тестовых данных, максимально приближенных к эксплуатационным.

## 15 Взаимоотношения с поставщиками

### 15.1 Информационная безопасность во взаимоотношениях с поставщиками

| |
|---|
| Цель: Обеспечить защиту активов организации, доступных поставщикам. |

#### 15.1.1 Политика информационной безопасности во взаимоотношениях с поставщиками

Мера обеспечения ИБ

Требования ИБ, направленные на снижение рисков, связанных с доступом поставщиков к активам организации, должны быть согласованы с поставщиком и задокументированы.

Руководство по применению

В своей политике организация должна определить и назначить меры обеспечения ИБ, которые относятся к доступу поставщиков к информации организации. Эти меры должны учитывать процессы и процедуры, которые должны выполняться организацией, а также те процессы и процедуры, которые организация должна требовать выполнять от поставщика, включая:

a) определение и документирование типов поставщиков, например ИТ-услуги, логистические услуги, финансовые услуги, компоненты ИТ-инфраструктуры, которым организация будет предоставлять доступ к своей информации;

b) стандартизированный процесс и жизненный цикл для управления отношениями с поставщиками;

c) определение типов доступа к информации, которые будут предоставлены различным типам поставщиков, а также мониторинг и контроль доступа;

d) минимальные требования по ИБ для каждой категории информации и типа доступа, учитывающие деловые потребности и требования организации, а также ее профиль рисков, которые будут служить основой для соглашений уже с конкретным поставщиком;

e) процессы и процедуры для контроля соблюдения установленных требований по ИБ для каждого типа поставщика и типа доступа, включая проверку третьей стороной и проверку продукта;

f) правильность и полноту мер обеспечения ИБ для обеспечения целостности информации или обработки информации, проводимой любой из сторон;

g) виды обязательств, применимых к поставщикам для защиты информации организации;

h) обработку инцидентов и непредвиденных обстоятельств, связанных с доступом поставщиков, включая обязанности как организации, так и поставщиков;

i) способность к восстановлению и, если необходимо, меры по восстановлению и устранению непредвиденных обстоятельств для обеспечения доступности информации или обработки информации, предпринимаемые любой из сторон;

j) обучение персонала организации, участвующего в закупках, действующим политикам, процессам и процедурам;

k) обучение персонала организации, взаимодействующего с персоналом поставщика, относительно соответствующих правил взаимодействия и поведения в зависимости от типа поставщика и уровня доступа поставщика к системам и информации организации;

l) условия, при которых требования и меры обеспечения ИБ будут включены в соглашение, подписанное обеими сторонами;

m) управление необходимой передачей информации, устройств обработки информации и чем-либо еще, нуждающимся в передаче, и гарантию того, что безопасность обеспечивается в течение всего периода передачи.

Дополнительная информация

При ненадлежащем управлении ИБ информация может подвергаться риску со стороны поставщиков. Должны быть определены и выполняться меры обеспечения ИБ для управления доступом поставщиков к средствам обработки информации. Например, если существует особая необходимость в сохранении конфиденциальности информации, может заключаться соглашение о неразглашении. Другой пример защиты данных от рисков — когда соглашение с поставщиками включает в себя вопросы передачи информации или доступа к информации из-за границы. Организация должна осознавать, что ответственность за соблюдение законодательства и контрактных обязательств по защите информации лежит на самой организации.

**15.1.2 Рассмотрение вопросов безопасности в соглашениях с поставщиками**

Мера обеспечения ИБ

Все соответствующие требования по ИБ должны быть установлены и согласованы с каждым поставщиком, который может получить доступ к информации организации, обрабатывать, хранить, передавать информацию или предоставлять соответствующие компоненты ИТ-инфраструктуры.

Руководство по применению

Соглашения с поставщиками должны быть разработаны и задокументированы, чтобы гарантировать, что между организацией и поставщиком нет недопонимания относительно взаимных обязательств по выполнению соответствующих требований по ИБ.

Для выполнения установленных требований ИБ следует рассмотреть включение в соглашения следующих условий:

a) описание предоставляемой информации или информации, к которой предоставляется доступ, а также методов предоставления информации или получения доступа к ней;

b) категории информации в соответствии с системой категорирования организации (см. 8.2); сопоставление, при необходимости, системы категорирования организации с системой категорирования поставщика;

c) законодательные и нормативные требования, включая требования по защите данных, прав на интеллектуальную собственность и авторских прав, а также описание того, как будет обеспечено их соблюдение;

d) обязательства каждой стороны договора по осуществлению согласованного набора мер обеспечения ИБ, включая управление доступом, анализ производительности, мониторинг, отчетность и аудит;

e) правила приемлемого использования информации, включая неприемлемое использование, в случае необходимости;

f) точный перечень персонала поставщика, который авторизован на доступ к информации или получение информации организации, либо процедуры или условия для назначения и аннулирования прав на доступ к информации или получение информации организации персоналом поставщика;

g) политики ИБ, относящиеся к конкретному договору;

h) требования и процедуры по управлению инцидентами (особенно уведомление и совместная работа по устранению последствий инцидентов);

i) требования к обучению и осведомленности о конкретных процедурах и требования к ИБ, например для реагирования на инциденты, процедуры авторизации;

j) соответствующие регламенты для субподряда, включая меры обеспечения ИБ, которые должны выполняться;

k) соответствующие партнеры по соглашению, включая контактное лицо по вопросам ИБ;

l) требования к предварительной проверке персонала поставщика, если таковые установлены, включая обязанности по проведению процедур предварительной проверки и информирования в случае, когда проверка не была завершена или ее результаты дают основания для сомнений или опасений;

m) право на аудит процессов поставщика и осуществление мер обеспечения ИБ, связанных с соглашением;

n) процессы устранения дефектов и разрешения конфликтов;

o) обязательство поставщика по периодическому предоставлению независимого отчета об эффективности мер обеспечения ИБ и соглашения о своевременном решении соответствующих проблем, упомянутых в отчете;

p) обязательства поставщика по соблюдению требований безопасности организации.

Дополнительная информация

Соглашения могут значительно различаться для разных организаций и разных типов поставщиков. В связи с этим следует уделить внимание тому, чтобы учесть все актуальные риски и требования ИБ. Соглашения с поставщиками могут также допускать участие других сторон (например, субподрядчиков).

В соглашении необходимо учесть процедуры обеспечения непрерывности производственных процессов в случае, если поставщик не в состоянии поставлять свои продукты или услуги, во избежание любых задержек из-за замены продуктов и услуг.

**15.1.3 Цепочка поставок информационно-коммуникационных технологий**

Мера обеспечения ИБ

Соглашения с поставщиками должны содержать требования по рассмотрению рисков ИБ, связанных с цепочкой поставок продуктов и услуг информационно-коммуникационных технологий.

Руководство по применению

Относительно безопасности цепочек поставок для включения в соглашения с поставщиками должны быть рассмотрены следующие положения:

a) определение требований ИБ, применимых к закупкам продуктов или услуг в области информационно-коммуникационных технологий, в дополнение к общим требованиям ИБ, относящимся к отношениям с поставщиками;

b) для услуг в области информационно-коммуникационных технологий требуется, чтобы поставщики распространяли требования безопасности организации на всю цепочку поставки, если поставщик привлекает подрядчиков для выполнения части услуг в области информационно-коммуникационных технологий, оказываемых организации;

c) для продуктов в области информационно-коммуникационных технологий требуется, чтобы поставщики распространяли соответствующие процедуры, связанные с безопасностью, на всю цепочку поставки, если эти продукты включают в себя компоненты, закупаемые у других поставщиков;

d) выполнение процесса мониторинга и подходящих методов для подтверждения того, что поставляемые продукты и услуги в области информационно-коммуникационных технологий соответствуют заявленным требованиям безопасности;

e) выполнение процесса определения компонентов продукта или услуги, которые являются критически важными для поддержания функциональности и следовательно требуют повышенного внимания и изучения, если произведены за пределами организации, особенно если первичный поставщик передает на аутсорсинг производство каких-то элементов продукта или услуги другим поставщикам;

f) получение уверенности в том, что критически важные компоненты и их происхождение могут быть прослежены по всей цепочке поставки;

g) получение уверенности в том, что поставляемые продукты в области информационно-коммуникационных технологий функционируют должным образом без каких-либо непредусмотренных или нежелательных функций;

h) определение правил обмена информацией, касающихся цепочки поставки и любых потенциальных проблем и компромиссов между организацией и поставщиками;

i) выполнение конкретных процессов управления жизненным циклом и доступностью компонентов информационно-коммуникационных технологий и связанными с ними рисками безопасности. Это включает в себя управление рисками, связанными с тем, что компоненты более не доступны в силу того, что их поставщики прекратили свою деятельность или прекратили поставку этих компонентов по причине развития технологий.

Дополнительная информация

Конкретные методы управления рисками в цепочке поставки информационно-коммуникационных технологий основаны на высокоуровневых процедурах обеспечения общей ИБ, качества, управления проектами и разработки систем, но не заменяют их.

Организациям рекомендуется работать с поставщиками для понимания цепочки поставки информационно-коммуникационных технологий и любых вопросов, оказывающих значительное влияние на поставляемые продукты и услуги. Организации могут влиять на методы обеспечения ИБ в цепочке поставок информационно-коммуникационных технологий, четко определяя в соглашениях со своими поставщиками вопросы, которые должны решаться другими поставщиками в цепочке поставок информационно-коммуникационных технологий.

Цепочка поставок информационно-коммуникационных технологий, как указано здесь, включает в себя услуги облачных вычислений.

### 15.2 Управление услугами, предоставляемыми поставщиком

Цель: Поддерживать согласованный уровень ИБ и предоставления услуги в соответствующих соглашениях с поставщиками.

#### 15.2.1 Мониторинг и анализ услуг поставщика

Мера обеспечения ИБ

Организации должны регулярно проводить мониторинг, проверку и аудит деятельности поставщика по предоставлению услуг.

Руководство по применению

Мониторинг и анализ услуг, предоставляемых поставщиком, должны обеспечивать уверенность в том, что положения и условия, касающиеся ИБ, отраженные в соглашениях, выполняются и что инциденты и проблемы в области ИБ решаются должным образом.

Это должно реализовываться при управлении услугами через процесс взаимодействия между организацией и поставщиком, чтобы:

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

b) анализировать отчеты об услугах, подготовленные поставщиком, и организовывать регулярные рабочие встречи, как это определено соглашениями;

c) проводить аудиты поставщиков вместе с анализом отчетов независимых аудиторов, если они есть, и осуществлять последующие действия по выявленным проблемам;

d) предоставлять информацию об инцидентах ИБ и анализировать эту информацию в соответствии с требованиями соглашений и любых вспомогательных методических рекомендаций и процедур;

e) анализировать контрольные записи поставщиков и записи о событиях безопасности, эксплуатационных проблемах, сбоях, обнаруженных ошибках и нарушениях, связанных с поставляемой услугой;

f) решать любые выявленные проблемы и управлять ими;

g) анализировать в разрезе аспектов ИБ отношения поставщика с его подрядчиками;

h) гарантировать, что поставщик сохраняет достаточную способность обслуживания согласно работоспособным планам, разработанным для обеспечения согласованных уровней непрерывности обслуживания при значительных сбоях и аварийных ситуациях (раздел 17).

Ответственность за управление отношениями с поставщиками следует возлагать на специально назначенное лицо или группу по управлению услугами. Кроме того, организация должна обеспечить, чтобы поставщики установили обязанности по анализу соответствия и обеспечению выполнения требований соглашения. Должны быть выделены достаточные ресурсы с необходимыми техническими навыками для мониторинга того, что требования соглашения, в частности требования ИБ, выполняются. Необходимо предпринимать соответствующие действия при обнаружении недостатков в оказании услуг.

Организация должна поддерживать достаточный общий контроль и прозрачность всех аспектов безопасности в отношении информации ограниченного доступа или устройств обработки информации, к которым поставщик имеет доступ, использует их или управляет ими. Организация должна поддерживать прозрачность действий, связанных с безопасностью, таких как управление изменениями, выявление уязвимостей, а также составление отчетов об инцидентах ИБ и реагирование на них с помощью установленного процесса оповещения.

#### 15.2.2 Управление изменениями услуг поставщика

Мера обеспечения ИБ

Требуется управлять изменениями в предоставляемых поставщиками услугах, включая поддержку и улучшение существующих политик, процедур, а также мер обеспечения ИБ, с учетом категории информации бизнеса, задействованных систем и процессов, а также результатов переоценки рисков ИБ.

Руководство по применению

Должны быть приняты во внимание следующие аспекты:

a) изменения в соглашениях с поставщиками;

b) изменения, проводимые организацией, для реализации:

1) улучшения текущих предлагаемых услуг;

2) разработки любых новых прикладных программ и систем;

3) изменения или обновления политик и процедур организации;

4) новых или измененных мер для устранения инцидентов ИБ и повышения безопасности;

c) изменения в услугах поставщика для реализации:

1) изменения и усовершенствования сетей;

2) использования новых технологий;

3) использования новых продуктов или новых версий/выпусков;

4) использования новых инструментов и сред разработки;

5) изменения физического расположения средств обслуживания;

6) смены поставщиков;

7) заключения контракта с другим субподрядчиком.

## 16 Менеджмент инцидентов информационной безопасности

### 16.1 Менеджмент инцидентов информационной безопасности и улучшений

Цель: Обеспечить последовательный и эффективный подход к менеджменту инцидентов ИБ, включая обмен информацией о событиях безопасности и недостатках.

#### 16.1.1 Обязанности и процедуры

Мера обеспечения ИБ

Должны быть установлены обязанности и процедуры менеджмента для обеспечения уверенности в быстром, эффективном и надлежащем реагировании на инциденты ИБ.

Руководство по применению

Должны быть приняты во внимание следующие рекомендации для обязанностей и процедур по управлению инцидентами ИБ:

a) должны быть установлены обязанности по управлению, чтобы гарантировать, что следующие процедуры разработаны и должным образом доведены до сведения внутри организации:

1) процедуры планирования и подготовки реагирования на инциденты;

2) процедуры мониторинга, обнаружения, анализа и информирования о событиях и инцидентах безопасности;

3) процедуры регистрации действий по управлению инцидентами;

4) процедуры обращения с криминалистическими свидетельствами;

5) оценка недостатков ИБ;

6) процедуры реагирования, включая процедуры эскалации, контролируемого восстановления после инцидента и информирования персонала внутри организации, лиц за ее пределами, а также организаций;

b) установленные процедуры должны обеспечивать, что:

1) вопросы, связанные с инцидентами ИБ в организации, решает компетентный персонал;

2) существуют контактные лица по вопросам обнаружения и информирования об инцидентах безопасности;

3) поддерживаются соответствующие контакты с органами власти, внешними заинтересованными группами или форумами, которые занимаются вопросами, связанными с инцидентами ИБ;

c) процедуры оповещения должны включать в себя:

1) подготовку форм оповещения о событиях безопасности для обеспечения действий по оповещению и для того, чтобы лица, сообщающие о нарушениях, могли запомнить все необходимые действия в случае, если произошло событие безопасности;

2) процедуру, которая должна быть предпринята в случае, если произошло событие ИБ, например немедленное фиксирование всех деталей, таких как вид несоответствия или нарушения, произошедший отказ, сообщения на экране и незамедлительное оповещение контактных лиц, а также принятие скоординированных действий;

3) ссылку на установленный формальный процесс принятия дисциплинарных мер к работникам, которые совершают нарушения безопасности;

4) соответствующие процессы обратной связи для обеспечения того, чтобы лица, сообщающие о событиях безопасности, были уведомлены о результатах после решения и закрытия проблемы.

Цели управления инцидентами ИБ должны быть согласованы с руководством и должны гарантировать, что лица, ответственные за управление инцидентами ИБ, понимают приоритеты организации при обработке инцидентов ИБ.

Дополнительная информация

Инциденты ИБ могут выходить за пределы организационных и национальных границ. Для реагирования на такие инциденты возрастает необходимость в координации и обмене информацией об этих инцидентах со сторонними организациями, в той мере, насколько это возможно.

Подробное руководство по управлению инцидентами ИБ приведено в ИСО/МЭК 27035 [20].

**16.1.2 Сообщения о событиях информационной безопасности**

Мера обеспечения ИБ

Требуется незамедлительно сообщать о событиях информационной безопасности по соответствующим каналам управления.

Руководство по применению

Все работники и подрядчики должны быть осведомлены о своей обязанности незамедлительно сообщать о событиях ИБ. Они должны быть также осведомлены о процедуре оповещения о событиях безопасности и контактных лицах, которым следует сообщать о событиях.

Ситуации, которые предполагают передачу сообщения о событии ИБ, включают в себя:

a) неэффективный контроль ИБ;

b) нарушение ожидаемого уровня целостности, конфиденциальности или доступности информации;

c) человеческие ошибки;

d) несоответствия политикам или руководствам;

e) нарушения мер физической безопасности;

f) неконтролируемые системные изменения;

g) неисправности программного или аппаратного обеспечения;

h) нарушения доступа.

Дополнительная информация

Сбои или иное ненормальное поведение системы могут быть индикаторами атак на систему защиты или фактического нарушения защиты, и следовательно о них всегда необходимо сообщать как о событиях ИБ.

**16.1.3 Сообщение о недостатках информационной безопасности**

Мера обеспечения ИБ

Работники и подрядчики, использующие информационные системы и услуги организации, должны обращать внимание на любые замеченные или предполагаемые недостатки ИБ в системах или сервисах и сообщать о них.

Руководство по применению

Все работники и подрядчики должны незамедлительно сообщать о недостатках ИБ контактных лиц, чтобы предотвратить инциденты ИБ. Механизм оповещения должен быть максимально простым, доступным и работоспособным.

Дополнительная информация

Работникам и подрядчикам должно быть рекомендовано не пытаться проверять предполагаемые недостатки безопасности. Тестирование недостатков может быть воспринято как потенциально неправильное использование системы, а также может повредить информационную систему или сервис и привести к юридической ответственности лица, выполняющего тестирование.

**16.1.4 Оценка и принятие решений в отношении событий информационной безопасности**

Мера обеспечения ИБ

Должна быть проведена оценка событий безопасности и принято решение, следует ли их классифицировать как инциденты ИБ.

Руководство по применению

Контактные лица по вопросам обнаружения и информирования об инцидентах должны оценивать каждое событие безопасности, используя согласованную шкалу классификации событий и инцидентов

безопасности, и решать, следует ли классифицировать событие как инцидент ИБ. Классификация и распределение инцидентов по приоритетам может помочь в определении влияния и масштаба инцидента.

В тех случаях, когда в организации есть группа реагирования на инциденты ИБ (ГРИИБ), оценка и принятие решения могут быть переданы ей для подтверждения или повторной оценки.

Результаты оценки и принятых решений должны быть подробно зафиксированы с целью обращения к ним в будущем и проверки.

**16.1.5 Реагирование на инциденты информационной безопасности**

Мера обеспечения ИБ

Реагирование на инциденты ИБ должно осуществляться в соответствии с документально оформленными процедурами.

Руководство по применению

Реагирование на инциденты ИБ должно осуществляться назначенными контактными лицами и другими соответствующими лицами из числа самой организации или сторонних организаций (см. 16.1.1).

Реагирование должно включать в себя следующее:

a) как можно более быстрый сбор свидетельств произошедшего;

b) проведение криминалистического анализа ИБ по мере необходимости (см. 16.1.7);

c) эскалация, если требуется;

d) обеспечение того, что все выполняемые действия по реагированию соответствующим образом зарегистрированы для дальнейшего анализа;

e) информирование о факте инцидента ИБ или любых существенных деталях о нем других лиц из числа самой организации или сторонних организаций в соответствии с принципом «необходимого знания»;

f) устранение недостатка(ов) ИБ, которые могут стать причиной или способствовать возникновению инцидента;

g) после того, как инцидент успешно отработан, необходимо формально закрыть и записать его.

После инцидента должен проводиться анализ для выявления первопричины инцидента.

Дополнительная информация

Первоочередной целью реагирования на инцидент является возобновление «нормального уровня безопасности», а затем инициирование необходимого восстановления.

**16.1.6 Извлечение уроков из инцидентов информационной безопасности**

Мера обеспечения ИБ

Знания, приобретенные в результате анализа и урегулирования инцидентов ИБ, должны использоваться для уменьшения вероятности или влияния будущих инцидентов.

Руководство по применению

Должны быть внедрены механизмы, позволяющие количественно определять и отслеживать типы, объемы и стоимость инцидентов ИБ. Информация, полученная в результате оценки инцидентов ИБ, должна использоваться для выявления повторяющихся или значительных инцидентов.

Дополнительная информация

Оценка инцидентов ИБ может указывать на необходимость в усилении или дополнении мер обеспечения ИБ для снижения частоты, ущерба и стоимости в будущем или может быть принята во внимание при пересмотре политики безопасности (см. 5.1.2).

При должном внимании к аспектам конфиденциальности, истории про реальные инциденты ИБ могут быть использованы при обучении персонала (см. 7.2.2) в качестве примеров того, что может случиться, как реагировать на такие инциденты и как избежать их в будущем.

**16.1.7 Сбор свидетельств**

Мера обеспечения ИБ

В организации должны быть определены и применяться процедуры для идентификации, сбора, получения и сохранения информации, которая может использоваться в качестве свидетельств.

Руководство по применению

Должны быть разработаны и затем выполняться внутренние процедуры при рассмотрении свидетельств с целью принятия мер дисциплинарного и юридического характера.

В общем случае эти процедуры должны обеспечивать процессы идентификации, сбора, получения и сохранения свидетельств в зависимости от типа носителей, устройств и состояния устройств, например включенных или выключенных. Процедуры должны учитывать:

a) цепочку поставок;

b) безопасность свидетельств;
c) безопасность персонала;
d) роли и обязанности задействованного персонала;
e) компетентность персонала;
f) документацию;
g) инструктаж.

Там, где это возможно, должна быть предусмотрена сертификация или другие соответствующие способы оценки квалификации персонала и инструментария для того, чтобы повысить ценность сохраненных свидетельств.

Криминалистические свидетельства могут выходить за пределы организации или границы юрисдикции. В таких случаях следует обеспечить, чтобы организация имела право собирать требуемую информацию в качестве криминалистических свидетельств. Должны быть учтены требования различных юрисдикций, чтобы максимально увеличить шансы на признание в соответствующих юрисдикциях.

Дополнительная информация

Идентификация — это процесс, включающий в себя поиск, распознавание и документирование возможного свидетельства. Сбор — это процесс сбора физических предметов, которые могут содержать потенциальные свидетельства. Получение — это процесс создания копии данных в рамках определенного набора. Сохранение — это процесс поддержания и защиты целостности и первоначального состояния потенциальных свидетельств.

Когда событие безопасности обнаружено впервые, может быть неясно, приведет ли это событие к судебному разбирательству. Следовательно, существует опасность, что необходимое свидетельство будет намеренно или случайно уничтожено до того, как выяснится серьезность инцидента. Рекомендуется заранее привлекать юриста или полицию к любым предполагаемым действиям юридического характера и прислушиваться к советам по поводу необходимых свидетельств.

ИСО/МЭК 27037 [24] содержит руководства по идентификации, сбору, получению и сохранению цифровых свидетельств.

## 17 Аспекты информационной безопасности в рамках менеджмента непрерывности деятельности организации

### 17.1 Непрерывность информационной безопасности

Цель: Непрерывность обеспечения ИБ должна быть неотъемлемой частью систем менеджмента непрерывности деятельности организации.

#### 17.1.1 Планирование непрерывности информационной безопасности

Мера обеспечения ИБ

Организация должна определить свои требования к ИБ и менеджменту непрерывности ИБ при неблагоприятных ситуациях, например во время кризиса или бедствия.

Руководство по применению

Организация должна определить, обеспечивается ли непрерывность ИБ в рамках процесса менеджмента непрерывностью бизнеса или в рамках процесса менеджмента восстановления после чрезвычайных ситуаций. Требования ИБ должны быть определены при планировании непрерывности бизнеса и восстановления после чрезвычайных ситуаций. При отсутствии формально утвержденных планов непрерывности бизнеса и восстановления после чрезвычайных ситуаций управление ИБ должно исходить из того, что требования ИБ в неблагоприятных ситуациях те же, что и при обычных условиях. В качестве альтернативы организация может провести анализ влияния на бизнес в разрезе аспектов ИБ, чтобы определить требования ИБ, которые применимы в неблагоприятных ситуациях.

Дополнительная информация

Чтобы сократить время и затраты на дополнительный анализ влияния на бизнес, рекомендуется учитывать аспекты ИБ в рамках обычного анализа влияния на менеджмент непрерывности бизнеса или восстановления после чрезвычайных ситуаций. Это предполагает, что требования к непрерывности ИБ четко сформулированы в процессах менеджмента непрерывности бизнеса или восстановления после чрезвычайных ситуаций. Информацию о менеджменте непрерывности бизнеса можно найти в ИСО 27031 [14], ИСО 22313 [9] и ИСО 22301 [8].

**17.1.2 Реализация непрерывности информационной безопасности**

Мера обеспечения ИБ

Организация должна установить, документировать, реализовать и поддерживать процессы, процедуры, а также меры для обеспечения требуемого уровня непрерывности ИБ при неблагоприятных ситуациях.

Руководство по применению

Организация должна обеспечить следующее:

a) наличие адекватной структуры управления по подготовке, реагированию и снижению последствий от неблагоприятных событий, включающей персонал, обладающий необходимым опытом, компетенциями и полномочиями;

b) утверждение ответственного персонала по реагированию на инциденты, обладающего необходимыми полномочиями и компетенциями, для управления инцидентами и обеспечения ИБ;

c) разработку и утверждение документированных планов, процедур реагирования и восстановления, подробно описывающих, как организация будет справляться с неблагоприятным событием и будет поддерживать ИБ на заранее определенном уровне, основанном на утвержденных руководством целях обеспечения непрерывности ИБ (см. 17.1.1).

В соответствии с требованиями непрерывности ИБ организация должна установить, задокументировать, реализовать и поддерживать:

a) меры обеспечения ИБ в процессах обеспечения непрерывности бизнеса или восстановления после аварийных ситуаций, процедуры, вспомогательные системы и инструменты;

b) процессы, процедуры и изменения для поддержания существующих мер обеспечения ИБ во время неблагоприятных ситуаций;

c) компенсирующие меры для тех мер обеспечения ИБ, которые не могут поддерживаться во время неблагоприятной ситуации.

Дополнительная информация

В контексте непрерывности бизнеса или восстановления после аварий могут быть определены конкретные процессы и процедуры. Информация, обрабатываемая в рамках этих процессов и процедур или поддерживающих информационных систем, должна быть защищена. Поэтому организация должна привлекать специалистов по ИБ при создании, внедрении и поддержке процессов и процедур обеспечения непрерывности бизнеса или восстановления после аварий.

Внедренные меры обеспечения ИБ должны оставаться работоспособными в неблагоприятных ситуациях. Если меры не могут продолжать выполнять свои функции по защите информации, следует определить, внедрить и поддерживать другие меры для обеспечения приемлемого уровня ИБ.

**17.1.3 Проверка, анализ и оценивание непрерывности информационной безопасности**

Мера обеспечения ИБ

Организация должна регулярно проверять установленные и реализованные меры по обеспечению непрерывности ИБ, чтобы обеспечить уверенность в их актуальности и эффективности при возникновении неблагоприятных ситуаций.

Руководство по применению

Организационные, технические, процедурные изменения или изменения в процессах как в контексте эксплуатации, так и непрерывности, могут привести к изменениям требований непрерывности ИБ. В таких случаях непрерывность процессов, процедур и мер обеспечения ИБ должна быть проанализирована с точки зрения изменений в требованиях.

Организации должны проверять непрерывность менеджмента ИБ путем:

a) осуществления и тестирования функциональности процессов, процедур и мер непрерывности ИБ для гарантии их соответствия целям обеспечения непрерывности ИБ;

b) осуществления и тестирования осведомленности и порядка управления процессами, процедурами и мерами непрерывности ИБ для гарантии того, что их выполнение соответствует целям обеспечения непрерывности ИБ;

c) анализа пригодности и эффективности мер непрерывности ИБ при изменении информационных систем, процессов, процедур и мер обеспечения ИБ или процессов и решений менеджмента непрерывности бизнеса/восстановления после аварий.

Дополнительная информация

Проверка мер непрерывности ИБ отличается от общей проверки ИБ и должна проводиться вне рамок тестирования изменений. По возможности желательно интегрировать проверку мер непрерывности ИБ в проверку непрерывности бизнеса организации или проверку восстановления после аварийной ситуации.

### 17.2 Резервирование оборудования

Цель: Обеспечить уверенность в доступности средств обработки информации.

#### 17.2.1 Доступность средств обработки информации

Мера обеспечения ИБ

Средства обработки информации должны быть внедрены с учетом резервирования, достаточного для выполнения требований доступности.

Руководство по применению

Организации должны определить требования бизнеса к доступности информационных систем. В тех случаях, когда доступность не может быть обеспечена существующей системной архитектурой, следует рассмотреть возможность добавления избыточности компонентам и архитектуре.

Там, где это применимо, обеспечивающие избыточность информационные системы должны быть проверены для гарантии того, что переключение с одного компонента на другой функционирует должным образом.

Дополнительная информация

Внедрение избыточности может порождать риски нарушения целостности или конфиденциальности информации и информационных систем. Их необходимо учитывать при проектировании информационных систем.

## 18 Соответствие

### 18.1 Соответствие правовым и договорным требованиям

Цель: Избежать нарушений правовых и регулятивных требований или договорных обязательств, связанных с ИБ, и других требований безопасности.

#### 18.1.1 Идентификация применимых законодательных и договорных требований

Мера обеспечения ИБ

Все соответствующие законодательные, нормативные, контрактные требования, а также подход организации к удовлетворению этих требований должны быть явным образом определены, документированы и сохраняться актуальными для каждой информационной системы и организации.

Руководство по применению

Конкретные меры и индивидуальные обязанности по выполнению этих требований также должны быть определены и задокументированы.

Руководство должно определить все законодательные акты, требования которых применимы к бизнесу организации и должны выполняться. Если организация ведет бизнес в нескольких странах, руководство должно учитывать требования каждой страны.

#### 18.1.2 Права на интеллектуальную собственность

Мера обеспечения ИБ

Должны быть реализованы соответствующие процедуры для обеспечения уверенности в соблюдении правовых, регулятивных и договорных требований, связанных с правами на интеллектуальную собственность и правами на использование проприетарных программных продуктов.

Руководство по применению

В отношении любых материалов, которые могут рассматриваться как интеллектуальная собственность, необходимо рассмотреть следующие рекомендации:

a) выпуск политики соблюдения прав на интеллектуальную собственность, которая определяет законное использование программного обеспечения и информационных продуктов;

b) приобретение программного обеспечения только у известных и доверенных источников для гарантии того, что авторское право не нарушается;

c) поддержание осведомленности о политике защиты прав интеллектуальной собственности и уведомление о намерении принять дисциплинарные меры в отношении нарушителей;

d) ведение соответствующих реестров активов и идентификация всех активов с требованиями по защите прав интеллектуальной собственности;

e) сохранение подтверждений и свидетельств прав собственности на лицензии, диски с дистрибутивами, руководства и т. д.;

f) внедрение мер обеспечения ИБ для гарантии того, чтобы не было превышено максимальное количество пользователей, установленное в рамках лицензии;

g) проведение проверок на предмет того, что установлено только авторизованное программное обеспечение и лицензионные продукты;

h) предоставление политики по поддержке соответствующих лицензионных соглашений;

i) предоставление политики по утилизации или передаче программного обеспечения другим лицам;

j) соблюдение условий использования программного обеспечения и информации, полученных из общедоступных сетей;

k) не дублировать, конвертировать и извлекать информацию из коммерческих записей (видео, аудио), если это нарушает законы об авторском праве;

l) не копировать полностью или частично книги, статьи, отчеты и другие документы, кроме разрешенных законом об авторском праве.

Дополнительная информация

Права на интеллектуальную собственность включают в себя авторское право на программное обеспечение или документы, права на проекты, торговые марки, патенты и лицензии на исходный код.

Проприетарные программные продукты обычно поставляются в соответствии с лицензионным соглашением, в котором указывают условия лицензии, например ограничение использования продукта конкретным компьютером или ограничение копирования только созданием резервных копий. Ситуацию в отношении прав на интеллектуальную собственность на программное обеспечение, разработанное организацией, следует разъяснить персоналу.

Законодательные, нормативные и договорные требования могут вводить ограничения на копирование материалов, являющихся предметом собственности. В частности, данные ограничения могут содержать требования на использование только тех материалов, которые разработаны организацией или предоставлены по лицензии, или переданы разработчикам для организации. Нарушение авторского права может привести к судебному иску, который может повлечь за собой штрафы и уголовное преследование.

**18.1.3 Защита записей**

Мера обеспечения ИБ

Записи должны быть защищены от потери, уничтожения, фальсификации, несанкционированного доступа и разглашения в соответствии с правовыми, регулятивными, договорными и бизнес-требованиями.

Руководство по применению

При принятии решения о защите определенных документов организации следует учитывать то, как они классифицированы по схеме организации. Записи должны быть разделены на типы, например бухгалтерские счета, записи баз данных, журналы транзакций, журналы событий и эксплуатационные процедуры. Для каждого из типов должен быть определен период хранения и допустимый носитель, например бумага, микрофиша, магнитная лента, оптические диски. Все криптографические ключи и программы, имеющие отношение к зашифрованным архивам или цифровым подписям (раздел 10), также должны сохраняться, чтобы обеспечить возможность расшифровывания записей во время их хранения.

Следует учитывать возможность порчи носителей, используемых для хранения записей. Процедуры их хранения и обработки должны осуществляться в соответствии с рекомендациями производителя.

Там, где выбираются электронные носители данных, должны быть установлены процедуры, обеспечивающие возможность доступа к данным (читаемость носителей и формата данных) в течение срока их хранения с целью защиты от потери в результате будущих изменений технологии.

Системы хранения данных следует выбирать таким образом, чтобы требуемые данные могли быть извлечены в приемлемые сроки и в приемлемом формате в зависимости от применимых требований.

Система хранения и обработки должна обеспечивать четкую идентификацию записей, а также период их хранения, установленный соответствующими национальными или региональными законами и нормами. Необходимо, чтобы эта система предоставляла возможность уничтожения документов после того, как у организации отпадет потребность в их хранении.

Для достижения целей защиты записей в организации должны быть предприняты следующие шаги:

a) должны быть выпущены руководящие принципы по срокам, хранению, обработке и утилизации записей и информации;

b) должен быть составлен график хранения с указанием записей и периода времени, в течение которого они должны храниться;

c) следует вести перечень источников ключевой информации.

Дополнительная информация

Может потребоваться обеспечение надежного хранения некоторых записей для соответствия законодательным, нормативным или договорным требованиям, а также для обеспечения основных видов деятельности бизнеса организации. Примерами являются записи, которые могут потребоваться в качестве доказательства того, что организация ведет деятельность в соответствии с законодательными и нормативными документами, для обеспечения защиты от потенциального гражданского или уголовного преследования, или для подтверждения финансового состояния организации акционерам, аудиторам и внешним сторонам. Национальное законодательство или нормативные акты могут устанавливать периоды времени и содержание данных для сохранения.

Дополнительную информацию о менеджменте записей организации можно найти в ИСО 15489-1 [5].

**18.1.4 Конфиденциальность и защита персональных данных**

Мера обеспечения ИБ

Конфиденциальность и защита персональных данных должна обеспечиваться в соответствии с требованиями соответствующих законодательных и нормативных актов там, где это применимо.

Руководство по применению

Должна быть разработана и внедрена политика организации в отношении конфиденциальности и защиты персональных данных. Эта политика должна быть доведена до сведения всех лиц, участвующих в обработке персональных данных.

Соблюдение этой политики и всех соответствующих законодательных актов и требований регуляторов, касающихся защиты неприкосновенности частной жизни людей и защиты персональных данных, требует подходящей структуры управления и контроля. Зачастую это лучше всего достигается назначением ответственного лица, такого как работника, ответственного за конфиденциальность, который должен предоставлять указания менеджерам, пользователям и поставщикам услуг относительно их индивидуальных обязанностей и конкретных процедур, которые они должны соблюдать. Ответственность за обработку персональных данных и обеспечение осведомленности о принципах конфиденциальности должна рассматриваться в соответствии с применимым законодательством и требованиями регуляторов. Должны быть приняты подходящие технические и организационные меры для защиты персональных данных.

Дополнительная информация

ИСО/МЭК 29100 [25] предоставляет высокоуровневую основу для защиты персональных данных в информационно-коммуникационных системах. Ряд стран ввели законодательство, устанавливающее контроль над сбором, обработкой и передачей персональных данных (как правило, это информация о живых людях, при помощи которой они идентифицируются). В зависимости от соответствующего национального законодательства, меры обеспечения ИБ могут налагать обязанности на тех, кто собирает, обрабатывает и распространяет персональные данные, а также могут ограничивать возможность их передачи в другие страны.

**18.1.5 Регулирование криптографических мер обеспечения информационной безопасности**

Мера обеспечения ИБ

Криптографические меры обеспечения информационной безопасности должны использоваться с соблюдением требований всех соответствующих соглашений, правовых и регулятивных актов.

Руководство по применению

Для соответствия применимым соглашениям, правовым актам и требованиям регуляторов, следует рассмотреть:

a) ограничения на импорт или экспорт компьютерного оборудования и программного обеспечения, выполняющего криптографические функции;

b) ограничения на импорт или экспорт компьютерного оборудования и программного обеспечения, спроектированного с учетом того, что в них могут быть добавлены криптографические функции;

c) ограничения на использование шифрования;

d) обязательные или добровольные методы доступа государственных органов к информации, зашифрованной с использованием аппаратного или программного обеспечения для обеспечения конфиденциальности информации.

Следует обратиться за юридической консультацией по вопросам соблюдения применимых законодательных и нормативных актов. Прежде, чем зашифрованная информация или криптографическое средство покинет границы юрисдикции, следует также получить юридическую консультацию.

### 18.2 Проверки информационной безопасности

Цель: Обеспечить уверенность в том, что ИБ реализована и эксплуатируется в соответствии с политикой и процедурами организации.

#### 18.2.1 Независимая проверка информационной безопасности

Мера обеспечения ИБ

Подход организации к менеджменту ИБ и ее реализация (т. е. цели, меры и средства, политики, процессы и процедуры ИБ) должны проверяться независимо друг от друга через запланированные интервалы времени или в случае значительных изменений.

Руководство по применению

Руководство должно инициировать проведение независимой проверки. Такая независимая проверка необходима для обеспечения постоянной пригодности, адекватности и эффективности подхода организации к управлению ИБ. Проверка должна включать оценку возможностей для улучшения и необходимости изменений в подходе к безопасности, включая задачи политики и мер обеспечения ИБ.

Такая проверка должна выполняться лицами, не связанными с проверяемой областью, например теми, кто проводит внутренние аудиты, независимыми руководителями или сторонними организациями, специализирующимися на проведении таких проверок. Лица, проводящие проверки, должны иметь соответствующие навыки и опыт.

Результаты независимой проверки должны быть задокументированы и доведены до сведения руководства, которое инициировало проверку. Эти записи должны сохраняться.

Если независимая проверка выявляет, что подход организации и реализация управления ИБ недостаточны, например документированные цели и требования не выполняются или не соответствуют направлению ИБ, установленному в политиках ИБ (см. 5.1.1), руководство должно рассмотреть необходимость корректирующих действий.

Дополнительная информация

ИСО/МЭК 27007 [12] «Руководство по аудиту систем управления информационной безопасностью» и ИСО/МЭК ТО 27008 [13] «Руководство для аудиторов по мерам обеспечения информационной безопасности» также предоставляют руководства для проведения независимой проверки.

#### 18.2.2 Соответствие политикам и стандартам безопасности

Мера обеспечения ИБ

Руководители, в пределах своей зоны ответственности, должны регулярно проверять соответствие процессов и процедур обработки информации соответствующим политикам ИБ, стандартам и любым другим требованиям безопасности.

Руководство по применению

Руководство должно определять, каким образом проверять соответствие требованиям ИБ, определенным в политиках, стандартах и других применимых нормативных актах. Необходимо рассмотреть возможность применения инструментов автоматизированного анализа и формирования отчетности для обеспечения эффективных регулярных проверок.

Если в результате проверки обнаружено несоответствие, руководству следует:

a) выявить причины несоответствия;

b) оценить необходимость выполнения действий для обеспечения соответствия;

c) принять соответствующие корректирующие меры;

d) проверить эффективность предпринятых корректирующих действий и выявить любые недостатки или слабости.

Результаты проверок и корректирующих действий, выполненных руководством, должны быть зафиксированы, а эти записи должны быть сохранены. Руководство должно сообщить о результатах лицам, проводящим независимые проверки (см. 18.2.1), когда проводится независимая проверка в области их ответственности.

Дополнительная информация

Применение систем оперативного мониторинга описано в 12.4.

**18.2.3 Анализ технического соответствия**

Мера обеспечения ИБ

Информационные системы должны регулярно проверяться на предмет соответствия стандартам и политикам ИБ организации.

Руководство по применению

Техническое соответствие должно проверяться предпочтительно с помощью автоматизированных инструментов, которые генерируют технические отчеты для последующей интерпретации техническим специалистом. Кроме этого, опытный системный инженер может проводить ручные проверки (с использованием соответствующих программных средств, при необходимости).

Если используются тесты на проникновение или оценка уязвимостей, следует проявлять осторожность, поскольку такие действия могут привести к нарушению безопасности системы. Такие тесты следует планировать, документировать и повторять.

Любая проверка технического соответствия должна проводиться только компетентными уполномоченными лицами или под их наблюдением.

Дополнительная информация

Проверки технического соответствия включают в себя экспертизу эксплуатируемых систем на предмет того, что аппаратные и программные меры обеспечения ИБ были правильно реализованы. Этот тип проверки соответствия требует наличия специалиста по технической экспертизе.

К проверкам соответствия относятся, например, тестирование на проникновение и оценка уязвимостей, которые могут проводиться независимыми экспертами, привлекаемыми на контрактной основе специально для этой цели. Это может быть полезным при обнаружении уязвимостей в системе и для проверки того, насколько эффективны меры обеспечения ИБ, направленные на предотвращение несанкционированного доступа, возможного вследствие использования этих уязвимостей.

Тесты на проникновение и оценка уязвимостей дают возможность получить мгновенный снимок системы в конкретном состоянии в конкретный момент времени. Снимок ограничен теми частями системы, которые фактически тестируются во время попытки(ок) осуществления проникновения. Тестирование на проникновение и оценка уязвимостей не заменяют оценку рисков.

ИСО/МЭК ТО 27008 [13] содержит конкретные рекомендации, связанные с проверками технического соответствия.

**Приложение ДА**
**(справочное)**

## Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

| Обозначение ссылочного международного стандарта | Степень соответствия | Обозначение и наименование соответствующего национального стандарта |
|---|---|---|
| ISO/IEC 27000 | — | * |

* Соответствующий национальный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык данного международного стандарта. Официальный перевод данного международного стандарта находится в Федеральном информационном фонде стандартов.

## Библиография


[1] ISO/IEC Directives, Part 2

[2] ISO/IEC 11770-1, Information technology Security techniques — Key management — Part 1: Framework

[3] ISO/IEC 11770-2, Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques

[4] ISO/IEC 11770-3, Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques

[5] ISO 15489-1, Information and documentation — Records management — Part 1: General

[6] ISO/IEC 20000-1, Information technology — Service management — Part 1: Service management system requirements

[7] ISO/IEC 20000-2, Information technology — Service management — Part 2: Guidance on the application of service management systems

[8] ISO 22301, Societal security — Business continuity management systems — Requirements

[9] ISO 22313, Societal security — Business continuity management systems — Guidance

[10] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

[11] ISO/IEC 27005, Information technology — Security techniques — Information security risk management

[12] ISO/IEC 27007, Information technology — Security techniques — Guidelines for information security management systems auditing

[13] ISO/IEC TR 27008, Information technology — Security techniques — Guidelines for auditors on information security controls

[14] ISO/IEC 27031, Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

[15] ISO/IEC 27033-1, Information technology — Security techniques — Network security — Part 1: Overview and concepts

[16] ISO/IEC 27033-2, Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security

[17] ISO/IEC 27033-3, Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues

[18] ISO/IEC 27033-4, Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways

[19] ISO/IEC 27033-5, Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Network (VPNs)

[20] ISO/IEC 27035, Information technology — Security techniques — Information security incident management

[21] ISO/IEC 27036-1, Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts
[22] ISO/IEC 27036-2, Information technology — Security techniques — Information security for supplier relationships — Part 2: Common requirements
[23] ISO/IEC 27036-3, Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for ICT supply chain security
[24] ISO/IEC 27037, Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence
[25] ISO/IEC 29100, Information technology — Security techniques — Privacy framework
[26] ISO/IEC 29101, Information technology — Security techniques — Privacy architecture framework
[27] ISO 31000, Risk management — Principles and guidelines

УДК 006.34:004.056:004.056.5:004.056.53:006.354 ОКС 35.030

Ключевые слова: информационная безопасность (ИБ), система менеджмента информационной безопасности (СМИБ), менеджмент риска, меры обеспечения ИБ

Редактор *Н.А. Аргунова*
Технический редактор *И.Е. Черепкова*
Корректор *О.В. Лазарева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 24.05.2021. Подписано в печать 08.06.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 8,37. Уч.-изд. л. 7,57.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru