МЕЖДУНАРОДНЫЙ СТАНДАРТ

**ISO/IEC 27001**

Вторая редакция
2013-10-01

# Информационные технологии - Методы защиты - Системы менеджмента информационной безопасности - Требования

*Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences*



Логотип ISO | Логотип IEC

Номер для ссылки
ISO/IEC 27001:2013 (E)

## ДОКУМЕНТ С ЗАЩИЩЕННЫМ АВТОРСКИМ ПРАВОМ

# Содержание

Страница

# Предисловие

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

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

Главная задача объединенного технического комитета состоит в том, чтобы разрабатывать международные стандарты. Проекты международных стандартов, принятые объединенным техническим комитетом, рассылаются национальным комитетам для голосования. Опубликование в качестве международного стандарта требует одобрения, по крайней мере, 75% национальных комитетов, имеющих право голоса.

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

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

Данная вторая редакция отменяет и заменяет первую редакцию (ISO/IEC 27001;2005), которая была подвергнута техническому пересмотру.

# 0 Введение

## 0.1 Общие положения

Настоящий Международный Стандарт был разработан с целью установить требования для создания, внедрения, поддержания функционирования и непрерывного улучшения системы менеджмента информационной безопасности. Признание необходимости системы менеджмента информационной безопасности является стратегическим решением организации. На создание и внедрение системы менеджмента информационной безопасности организации влияют потребности и цели организации, требования по безопасности, применяемые организационные процессы, размер и структура организации. Все эти факторы влияния ожидаемо меняются в течение длительного времени.

Система менеджмента информационной безопасности направлена на сохранение конфиденциальности, целостности и доступности информации за счет применения процессов управления рисками и обеспечивает уверенность заинтересованных сторон в том, что риски управляются надлежащим образом.

Важно то, что система менеджмента информационной безопасности составляет часть процессов организации и встроена в общую структуру управления, и, таким образом, вопросы информационной безопасности учитываются при разработке процессов, информационных систем и средств управления. Предполагается, что система менеджмента информационной безопасности будет меняться в соответствии с потребностями организации.

Настоящий Международный Стандарт может использоваться как самой организацией, так и внешними сторонами для оценки способности организации соответствовать собственным требованиям по информационной безопасности.

Порядок, в котором изложены требования представлены в Настоящем Международном Стандарте, не отражают их важности или последовательности, в которой они должны внедряться. Нумерация пунктов введена исключительно для удобства ссылок на них.

ISO/IEC 27000 содержит общий обзор и словарь терминов для систем менеджмента информационной безопасности, а также ссылки на соответствующие термины и определения, данные в серии стандартов по системам менеджмента информационной безопасности, включая ISO/IEC 27003 [2], ISO/IEC 27004 [3] и ISO/IEC 27005 [4].

## 0.2 Совместимость с другими стандартами системы управления

Настоящий Международный Стандарт следует структуре высшего уровня, содержит идентичные заголовки подразделов, идентичный текст, общие термины и основные определения, установленные в Части 1 Приложения SL Директивы ISO/IEC, Consolidated ISO Supplement, и, тем самым, обеспечивается совместимость с другими стандартами на системы менеджмента, которые соответствуют Приложению SL.

Такой общий подход, определенный в Приложении SL, будет полезен для тех организаций, которые хотят оперировать единой системой менеджмента, отвечающей требованиям двух или более стандартов на системы менеджмента.

# Информационные технологии - Методы защиты - Система менеджмента информационной безопасности - Требования

## 1 Область применения

Настоящий Международный Стандарт определяет требования к созданию, внедрению, поддержанию функционирования и непрерывному улучшению системы менеджмента информационной безопасности в рамках контекста организации. Настоящий Международный Стандарт также включает требования для оценки и обработки рисков информационной безопасности, адаптированные к потребностям организации. Требования, установленные Настоящим Международным Стандартом, являются общими и предназначены для применения любыми организациями, независимо от их типа, размера или характера. Не допускается исключений требований, установленных в разделах 4 – 10, в тех случаях, когда организация декларирует соответствие требованиям Настоящего Международного Стандарта.

## 2 Нормативные ссылки

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

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

## 3 Термины и определения

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

## 4 Контекст организации

### 4.1 Понимание организации и ее контекста

Организация должна определить внешние и внутренние проблемы, которые значимы с точки зрения ее целей, и которые влияют на способность ее системы менеджмента информационной безопасности достигать ожидаемых результатов.

ПРИМЕЧАНИЕ При определении этих проблем воспользуйтесь положениями об установлении внешнего и внутреннего контекста организации, содержащимися в разделе 5.3 ISO 31000:2009 [5].

### 4.2 Понимание потребностей и ожиданий заинтересованных сторон

Организация должно определить:

a) заинтересованные стороны, которые имеют существенное отношение к системе менеджмента информационной безопасности; и

b) требования этих заинтересованных сторон, относящиеся к информационной безопасности.

ПРИМЕЧАНИЕ Требования заинтересованных сторон могут включать законодательные и нормативные требования и договорные обязательства.

### 4.3 Определение области применения системы менеджмента информационной безопасности

Организация должна определить границы и применимость системы менеджмента информационной безопасности, чтобы установить ее область применения.

Определяя эту область, организация должна принять во внимание:

a) внешние и внутренние проблемы, упомянутые в разделе 4.1;

b) требования, упомянутые в разделе 4.2; и

c) взаимосвязи и зависимости между действиями, выполняемыми организацией, и теми, что выполняются другими организациями.

Область применения должна быть оформлена как документированная информация.

### 4.4 Система менеджмента информационной безопасности

Организация должна установить, внедрить, поддерживать функционирование и непрерывно улучшать систему менеджмента информационной безопасности в соответствии с требованиями Настоящего Международного Стандарта.

## 5 Лидерство

### 5.1 Лидерство и обязательства

Высшее руководство должно демонстрировать лидерство и обязательства в отношении системы менеджмента информационной безопасности посредством:

a) обеспечения того, что информационная политика безопасности и цели в сфере информационной безопасности установлены и согласуются со стратегией организации;

b) обеспечения встраивания требований системы менеджмента информационной безопасности в процессы организации;

c) обеспечения доступности ресурсов, необходимых для системы менеджмента информационной безопасности;

d) донесения важности результативного управления информационной безопасностью и соответствия требованиям системы менеджмента информационной безопасности;

e) обеспечения достижения системой менеджмента информационной безопасности ожидаемых результатов;

f) поддержки усилий сотрудников, направленных на обеспечение результативности системы менеджмента информационной безопасности;

g) стимулирования непрерывного совершенствования; и

h) поддержки демонстрации лидерства всеми иными исполняющими значимые управленческие функции в рамках их сферы ответственности.

### 5.2 Политика

Высшее руководство должно установить политику информационной безопасности, которая:

a) соответствует назначению организации;

b) включает целевые показатели в сфере информационной безопасности, (см. раздел 6.2) или служит основой для задания таких показателей;

c) включает обязательство соответствовать применимым требованиям, связанные с информационной безопасностью; и

d) включает обязательство непрерывного улучшения системы менеджмента информационной безопасности.

Политика информационной безопасности должна:

e) быть оформлена как документированная информация;

f) быть распространена в организации; и

g) быть доступной в установленном порядке для заинтересованных сторон.

### 5.3 Организационные функции, ответственность и полномочия

Высшее руководство должно гарантировать, что для функций, существенных с точки зрения информационной безопасности, ответственность и полномочия назначены и доведены до сведения.

Высшее руководство должно установить ответственность и полномочия для:

a) обеспечения соответствия системы менеджмента информационной безопасности требованиям Настоящего Международного Стандарта ; и

b) отчета о функционировании системы менеджмента информационной безопасности высшему руководству.

ПРИМЕЧАНИЕ Высшее руководство может также возложить ответственность и дать полномочия для информирования о функционировании системы менеджмента информационной безопасности в рамках организации.

## 6 Планирование

### 6.1 Действия в отношении рисков и потенциальных возможностей

#### 6.1.1 Общие положения

Планируя систему менеджмента информационной безопасности, организация должна принять во внимание проблемы, упомянутые в разделе 4.1 и требования, установленные в разделе 4.2, а также определить риски и потенциальные возможности, которые необходимо принять во внимание, чтобы:

a) гарантировать, что система менеджмента информационной безопасности может достигать ожидаемых результатов;

b) предотвратить или уменьшить нежелательные эффекты; и

c) достичь непрерывного совершенствования.

Организация должна планировать:

d) действия в отношении этих рисков и потенциальных возможностей; и

e) каким образом

1) встраивать эти действия в процессы системы менеджмента информационной

безопасности и осуществлять их; и

2) оценивать результативность этих действий.

### 6.1.2 Оценка рисков информационной безопасности

Организация должна определить и применять процесс оценки рисков информационной безопасности, который:

a) устанавливает и обеспечивает применение критериев оценки информационной безопасности, включающие в себя:

1) критерии приемлемости риска; и

2) критерии для осуществления оценки рисков информационной безопасности;

b) гарантирует, что производимые оценки рисков информационной безопасности дают непротиворечивые, обоснованные и сопоставимые результаты;

c) обеспечивает выявление рисков информационной безопасности:

1) включает в себя процесс оценки рисков информационной безопасности, направленный на идентификацию рисков, связанных с потерей конфиденциальности, целостности и доступности информации в рамках области применения системы менеджмента информационной безопасности; и

2) обеспечивает определение владельцев риска;

d) обеспечивает анализ рисков информационной безопасности:

1) оценку потенциальных последствий в том случае, если бы риски, идентифицированные при выполнении требований п. 6.1.2. c) 1) реализовались;

2) оценку реальной вероятности реализации рисков, идентифицированных при выполнении требований п. 6.1.2. c) 1); и

3) определение уровней риска;

e) обеспечивает оценку рисков информационной безопасности:

1) сравнение результатов анализа рисков с критериями риска, установленными при выполнении требований п. 6.1.2. a); и

2) расстановку рисков по приоритетам для последующей обработки рисков.

Организация должна сохранять данные процесса оценки рисков информационной безопасности как документированную информацию.

### 6.1.3 Обработка рисков информационной безопасности

Организация должна определить и выполнять процесс обработки рисков информационной безопасности с целью:

a) выбрать соответствующие методы обработки рисков информационной безопасности с учетом результатов оценки рисков;

b) определить любые средства управления, которые необходимы для реализации выбранных методов обработки рисков информационной безопасности;

ПРИМЕЧАНИЕ Организации могут самостоятельно разрабатывать средства управления или взять их из любого источника.

c) сравнить средства управления, определенные при выполнении требований п. 6.1.3 b), с приведенными в приложении A, и удостовериться, что никакие из необходимых средств управления не были пропущены;

ПРИМЕЧАНИЕ 1 Приложение A содержит полный перечень задач и соответствующих средств

управления для их реализации. Пользователям Настоящего Международного Стандарта следует использовать Приложение А с тем, чтобы гарантировать, что никакие необходимые средства управления не были пропущены.

ПРИМЕЧАНИЕ 2 Выбранные средства управления косвенным образом определяют и задачи управления. Задачи и средства управления, перечисленные в Приложении А, не являются исчерпывающими и могут потребоваться дополнительные задачи и средства управления.

d) сформировать Заявление о Применимости, которое содержит необходимые средства управления (см.6.1.3 b) и c)) и информацию по каждому выбранному средству управления, применяется ли оно в настоящий момент или нет, а также обоснование исключения средств управления, приведенных в Приложении А;

e) разработать план обработки рисков информационной безопасности; и

f) получить одобрение плана от владельцев риска и подтверждение принятия остаточных рисков информационной безопасности.

Организация должна сохранять данные процесса обработки рисков информационной безопасности как документированную информацию.

ПРИМЕЧАНИЕ Процессы оценки и обработки рисков информационной безопасности в Настоящем Международном Стандарте согласуются с принципами и общими руководящими указаниями, приведенными в ISO 31000 [5].

### 6.2 Целевые показатели в сфере информационной безопасности и планирование их достижения

Организация должна установить целевые показатели в сфере информационной безопасности для соответствующих функций и уровней.

Целевые показатели в сфере информационной безопасности должны:

a) быть согласованными с политикой информационной безопасности;

b) быть измеримыми (если достижимы);

c) учитывать применимые требования к информационной безопасности, а также результаты оценки и обработки рисков;

d) быть сообщены персоналу; и

e) соответствующим образом обновляться.

Организация должна сохранять данные по целевым показателям информационной безопасности как документированную информацию.

При планировании, каким образом достигнуть своих целевых показателей информационной безопасности, организация должна определить:

f) что должно быть сделано;

g) какие потребуются ресурсы;

h) кто будет нести ответственность;

i) когда ожидается завершение; и

j) каким образом будут оценены результаты.

## 7 Обеспечение

### 7.1 Ресурсы

Организация должна определить и обеспечить ресурсы, необходимые для разработки,

внедрения, поддержания функционирования и непрерывного улучшения системы менеджмента информационной безопасности.

## 7.2 Компетентность

Организация должна:

a) определять необходимую компетентность персонала, который выполняет работу под управлением организации, и который влияет на ее информационную безопасность;

b) гарантировать, что этот персонал компетентен в силу соответствующего образования, подготовки или опыта;

c) там, где это возможно, предпринимать меры для обеспечения необходимой компетентности и оценивать результативность предпринятых мер; и

d) сохранять соответствующую документированную информацию как доказательства компетентности.

ПРИМЕЧАНИЕ Возможные действия могут включать, например: обучение, наставничество или перемещение работающих сотрудников; или прием новых или привлечение по контракту компетентных специалистов.

## 7.3 Осведомленность

Персонал, выполняющий работу в рамках системы управления организации, должен знать:

a) политику в области информационной безопасности,

b) их вклад в результативность системы менеджмента информационной безопасности, включая выгоды от улучшения деятельности по обеспечению информационной безопасности, и

c) последствия несоответствий требованиям системы менеджмента информационной безопасности.

## 7.4 Коммуникация

Организация должна определить потребность во внутренних и внешних коммуникациях, существенных для функционирования системы менеджмента информационной безопасности, включая:

a) на какой предмет обмениваться информацией,

b) когда обмениваться информацией;

c) с кем обмениваться информацией;

d) кто должен обмениваться информацией; и

e процессы, посредством которых должна производиться коммуникация.

## 7.5 Документированная информация

### 7.5.1 Общие положения

Система менеджмента информационной безопасности организации должна включать:

a) документированную информацию, требуемую Настоящим Международным Стандартом; и

b) документированную информацию, признанную организацией необходимой для обеспечения результативности системы менеджмента информационной безопасности.

ПРИМЕЧАНИЕ Объем документированной информации системы менеджмента информационной безопасности может отличаться в разных организациях в силу

1) размера организации и вида ее деятельности, процессов, продуктов товаров и услуг,

2) сложности процессов и их взаимодействия и

3) компетентности персонала.

### 7.5.2 Создание и обновление

Создавая и обновляя документированную информацию организация должна обеспечить соответствующие

a) идентификацию и выходные данные (например, название, дата, автор или ссылочный номер),

b) формат (например, язык, версия программного обеспечения, графики) и носитель (например, бумага, электронный вид),

c) пересмотр и утверждение в целях сохранения пригодности и соответствия.

### 7.5.3 Управление документированной информацией

Документированной информацией, требуемой системой менеджмента информационной безопасности и Настоящим Международным Стандартом, необходимо управлять, чтобы гарантировать, что она

a) доступна и пригодна для применения, где и когда она необходима, и

b) надлежащим образом защищена (например, от потери конфиденциальности, неправильного использования или потери целостности).

Для управления документированной информацией организация должна осуществлять следующие действия, насколько это применимо

a) рассылать, обеспечивать доступ, выдачу и применение,

b) хранить и сохранять в надлежащем состоянии, включая сохранение четкости,

c) контролировать изменения (например, контроль версий) и

d) устанавливать срок хранения и методы уничтожения.

Документированная информация внешнего происхождения, признанная организацией необходимой для планирования и функционирования системы менеджмента качества, должна быть идентифицирована соответствующим образом и управляться.

ПРИМЕЧАНИЕ Доступ подразумевает решение относительно разрешения только просматривать документированную информацию или разрешения и полномочий просматривать и изменять документированную информацию и т.д.

# 8 Функционирование

## 8.1 Планирование и управление функционированием

Организация должна планировать, осуществлять и управлять процессами, необходимыми для обеспечения соответствия требованиям, и выполнять действия, определенные в п. 6.1. Организация должна также выполнять запланированные действия для достижения целевых показателей, определенных в п.6.2

Организация должна сохранять документированную информацию в объеме, необходимом для обеспечения уверенности, что процессы были выполнены как запланировано.

Организация должна управлять запланированными изменениями и анализировать последствия непреднамеренных изменений, принимая, по мере необходимости, меры для снижения любых отрицательные воздействий.

Организация должна гарантировать, что переданные для выполнения на сторону процессы

определены и управляются.

### 8.2 Оценка рисков информационной безопасности

Организация должна выполнять оценку рисков информационной безопасности с учетом критериев, установленных в 6.1.2 a), через запланированные интервалы времени или когда предложены или произошли существенные изменения.

Организация должна сохранять результаты оценки рисков информационной безопасности как документированную информацию.

### 8.3 Обработка рисков информационной безопасности

Организация должна осуществлять план обработки рисков информационный безопасности.

Организация должна сохранять результаты обработки рисков информационной безопасности как документированную информацию.

## 9 Оценка результатов деятельности

### 9.1 Мониторинг, измерение, анализ и оценка

Организация должна оценивать обеспечение информационной безопасности и результативность системы менеджмента информационной безопасности.

Организация должна определить:

a) что должно быть объектом мониторинга и измерений, включая процессы и средства управления информационной безопасностью;

b) методы мониторинга, измерения, анализа и оценки, насколько это применимо, чтобы гарантировать пригодные результаты;

ПРИМЕЧАНИЕ Выбранные методы, чтобы считаться пригодными, должны давать сопоставимые и воспроизводимые результаты.

c) когда должен выполняться мониторинг и измерения;

d) кто должен осуществлять мониторинг и измерения;

e) когда результаты мониторинга и измерений должны анализироваться и оцениваться; и

f) кто должен анализировать и оценивать эти результаты.

Организация должна сохранять результаты мониторинга и измерений как документированную информацию.

### 9.2 Внутренний аудит

Организация должна проводить внутренние аудиты через запланированных интервалы времени, чтобы получать информацию о том,

a) соответствует ли система менеджмента информационной безопасности

1) собственным требованиям организации к ее системе менеджмента информационной безопасности; и

2) требованиям Настоящего Международного Стандарта;

b) что система менеджмента качества результативно внедрена и функционирует.

Организация должна:

c) планировать, выполнять и управлять программой(ами) аудитов, включая периодичность их проведения, методы, ответственность, требования к планированию и отчетности. Программа (ы) аудитов должна учитывать значимость проверяемых процессов и

результаты предыдущих аудитов;

d) определить критерии и область аудита для каждой проверки;

e) выбирать аудиторов и проводить аудиты так, чтобы гарантировать объективность и беспристрастность процесса аудита;

f) гарантировать, что результаты аудитов переданы на соответствующие уровни управления для оценки,

g) сохранять программу аудита и его результаты как документированную информацию.

### 9.3 Анализ системы руководством

Высшее руководство должно анализировать систему менеджмента информационной безопасности организации через запланированные интервалы времени, чтобы гарантировать ее постоянную пригодность, соответствие и результативность.

При анализе руководства необходимо учитывать следующее:

a) статус мероприятий, предусмотренных предыдущим анализом;

b) изменения в состоянии внешних и внутренних проблемных вопросов, которые относятся к системе менеджмента информационной безопасности;

c) информация о функционировании системы менеджмента информационной безопасности, включая тенденции в:

   1) несоответствиях и корректирующих действиях;

   2) результатах мониторинга и измерений;

   3) результатах аудитов; и

   4) достижении целевых показателей информационной безопасности;

d) обратную связь от заинтересованных сторон;

e) результаты оценки рисков и статус выполнения плана обработки рисков; и

f) потенциальные возможности для постоянного улучшения.

Результаты анализа должны включать решения, связанные с возможностями непрерывного улучшения и любыми потребностями в изменениях системы менеджмента информационной безопасности.

Организация должна сохранить результаты анализа системы руководством как документированную информацию.

## 10 Улучшение

### 10.1 Несоответствия и корректирующие действия

При выявлении несоответствия организация должна:

a) реагировать на несоответствие и, насколько применимо:

   1) принять меры для управления им и его исправления; и

   2) принять меры в отношении последствий;

b) оценивать потребность в действиях по устранению причины несоответствия с тем, чтобы оно не повторялось или не происходило в другом месте, посредством:

   1) анализа несоответствия;

   2) определения причин несоответствий, и

   3) выявления, есть ли подобные несоответствия, или могли бы они потенциально

произойти;

c) осуществлять любое необходимое действие;

d) анализировать результативность всех предпринятых корректирующих действий; и

e) вносить изменения в систему менеджмента информационной безопасности, если необходимо.

Корректирующие действия должны соответствовать последствиям выявленных несоответствий.

Организация должна сохранять данные о:

f) характере несоответствий и любых последующих предпринятых мер; и

g) результатах любого корректирующего действия

как документированную информацию.

## 10.2 Непрерывное улучшение

Организация должна непрерывно улучшать пригодность, соответствие и результативность системы менеджмента информационной безопасности.

# Приложение А
(нормативное)
# Связь задач и средств их реализации

Задачи и средства их реализации, перечисленные в Приложении А непосредственно взяты и согласуются с теми, что перечислены в разделах 5 - 18 ISO/IEC 27002:2013 [1] и должны применяться в контексте п. 6.1.3.

**Таблица А.1 - Задачи и средства их реализации**

| | | |
|---|---|---|
| **А.5 Политики информационной безопасности** | | |
| **А.5.1 Направляющая роль руководства в сфере информационной безопасности** | | |
| Задача: обеспечить направляющую роль менеджмента и поддержку информационной безопасности в соответствии с требованиями бизнеса и соответствующими законодательными и регламентирующими требованиями. | | |
| А5.1.1. | Политики информационной безопасности | *Средства реализации*<br>Должен быть разработан, одобрен руководством, опубликован и доведен до персонала и соответствующих внешних сторон комплекс политик информационной безопасности. |
| А.5.1.2 | Пересмотр политики информационной безопасности | *Средства реализации*<br>С тем, чтобы гарантировать постоянную пригодность, соответствие и результативность политик информационной безопасности, они должны пересматриваться через запланированные интервалы времени или когда произведены существенные изменения. |
| **А.6 Организация системы информационной безопасности** | | |
| **А.6.1 Внутренняя организация** | | |
| Задача: создать управленческую инфраструктуру, которая бы инициировала и управляла внедрением и функционированием системы информационной безопасности в рамках организации. | | |
| А.6.1.1 | Роли и ответственность в системе информационной безопасности | *Средства реализации*<br>Должна быть определена и назначена вся необходимая для системы информационной безопасности ответственность. |
| А.6.1.2 | Разделение обязанностей | *Средства реализации*<br>Для снижения риска несанкционированного или неумышленного изменения или неправильного применения активов организации должны быть разделены конфликтующие между собой обязанности и области ответственности. |

| | | |
|---|---|---|
| A.6.1.3 | Контакты с полномочными органами | *Средства реализации*<br>Должны поддерживаться соответствующие контакты с полномочными органами. |
| A.6.1.4 | Контакты с профессиональными сообществами | *Средства реализации*<br>Должны поддерживаться соответствующие контакты со специализированными общественными группами или иными форумами специалистов по безопасности, а также с профессиональными ассоциациями. |
| A.6.1.5 | Информационная безопасность в управлении проектами | *Средства реализации*<br>Требования по информационной безопасности должны применяться и к управлению проектами, независимо от типа проекта. |
| **A.6.2 Мобильные устройства и удаленная работа** | | |
| Задача: гарантировать безопасность при удаленной работе и использовании мобильных устройств. | | |
| A.6.2.1 | Политика в отношении мобильных устройств | *Средства реализации*<br>Должны быть приняты политика и меры по обеспечению безопасности, чтобы управлять рисками, связанными с использованием мобильных устройств. |
| A.6.2.2 | Удаленная работа | *Средства реализации*<br>Должны быть приняты политика и меры по обеспечению безопасности, чтобы защитить информацию, к которой имеется доступ, которая обрабатывается или сохраняется на ресурсах, используемых для удаленной работы. |
| **A.7 Безопасность, связанная с персоналом** | | |
| **A.7.1 До приема на работу** | | |
| Задача: гарантировать, что сотрудники и нанимаемые по контракту понимают свои обязанности и подходят для предполагаемой для них роли. | | |
| A.7.1.1 | Проверка | *Средства реализации*<br>Должна выполняться предварительная проверка всех кандидатов, принимаемых на работу в рамках соответствующих законов, регламентов и этических норм, а также соответствующая деловым требованиям, предъявляемым к кандидату, категории информации, которая ему будет доступна, и предполагаемых рисков. |
| A.7.1.2 | Обязательства в трудовом соглашении | *Средства реализации*<br>Трудовой договор (контракт) с сотрудниками и привлекаемыми со стороны исполнителями должен устанавливать как их обязательства, связанные с информационной безопасностью, так и обязательства организации. |

| | | |
|---|---|---|
| **A.7.2 В период работы** | | |
| Задача: гарантировать, что сотрудники и привлеченные по контракту знают и выполняют свои обязательства, связанные с информационной безопасностью. | | |
| A.7.2.1 | Ответственность руководства | *Средства реализации*<br>Руководство должно требовать от всех сотрудников и работающих по контракту соблюдения требований по информационной безопасности, в соответствии с установленными политиками и процедурами организации. |
| A.7.2.2 | Знание требований по информационной безопасности, образование и обучение | *Средства реализации*<br>Для всех сотрудников организации и, где это применимо, работающих по контракту должны быть проведены обучение и подготовка, обеспечивающие соответствующие знания, а также регулярное обновление организационных политик и процедур в той мере, в какой это касается их служебных обязанностей. |
| A.7.2.3 | Дисциплинарные взыскания | *Средства реализации*<br>Должны быть установлены и доведены до сведения всех на местах регламентированные действия, которые будут предприняты к нарушителям правил информационной безопасности. |
| **A.7.3 Прекращение и изменение трудовых отношений** | | |
| Задача: защитить интересы организации в случае прекращения или изменения трудовых отношений. | | |
| A.7.3.1 | Прекращение или изменение обязательств сотрудника | *Средства реализации*<br>Должны быть определены и доведены до сведения сотрудника или работающего по контракту его обязательства и обязанности в отношении информационной безопасности, сохраняющие свое действие после прекращения или изменения трудовых отношений, а также обеспечено их выполнение. |
| **A.8 Управление активами** | | |
| **A.8.1 Ответственность за активы** | | |
| Задача: идентифицировать активы организации и определить соответствующую ответственность, связанную с их защитой. | | |
| A.8.1.1 | Инвентаризация активов | *Средства реализации*<br>Активы, связанные с информацией и устройствами обработки информации должны быть идентифицированы, реестр таких активов должен быть составлен и поддерживаться в актуальном состоянии. |
| A.8.1.2 | Владельцы активов | *Средства реализации*<br>Активам, включенным в реестр, должны быть назначены |

| | | |
|---|---|---|
| | | владельцы. |
| A.8.1.3 | Надлежащее использование активов | *Средства реализации*<br>Правила для надлежащего использования информации и активов, связанных с информацией и устройствами обработки информации должны быть определены, документированы и внедрены. |
| A.8.1.4 | Возврат активов | *Средства реализации*<br>Все сотрудники и сторонние пользователи должны вернуть все активы организации в ее распоряжение по окончании действия трудовых соглашений. |
| **A.8.2 Классификация информации** | | |
| Задача: гарантировать, что информация имеет уровень защиты, соответствующий ее значимости для организации. | | |
| A.8.2.1 | Классификация информации | *Средства реализации*<br>Информация должна быть классифицирована с точки зрения законодательных требований, значимости, критичности и чувствительности к неавторизованному раскрытию или изменению. |
| A.8.2.2 | Маркировка информации | *Средства реализации*<br>Должен быть разработан и внедрен набор процедур для идентификации информации в соответствии с принятой в организации классификацией. |
| A.8.2.3 | Управление активами | *Средства реализации*<br>Должны быть разработаны и внедрены процедуры для управления активами в соответствии с принятой в организации классификацией информации. |
| **A.8.3 Управление носителями информации** | | |
| Задача: предотвратить несанкционированное раскрытие, изменение, удаление или порчу информации, хранящейся на определенном носителе. | | |
| A.8.3.1 | Управление съемными носителями | *Средства реализации*<br>Должны быть внедрены процедуры управления сменными носителями в соответствии с принятой в организации классификацией информации. |
| A.8.3.2 | Утилизация носителей информации | *Средства реализации*<br>Носители информации должны в соответствии с формальными процедурами надежно уничтожаться после того, как в них отпала надобность. |
| A.8.3.3 | Физическое перемещение носителей информации | *Средства реализации*<br>Носители информации во время транспортировки должны быть защищены от неавторизованного доступа, нецелевого использования или повреждения. |

| | | |
|---|---|---|
| **A.9 Управление доступом** | | |
| **A.9.1 Требования к управлению доступом, устанавливаемые бизнесом** | | |
| Задача: ограничить доступ к информации и устройствам ее обработки. | | |
| A.9.1.1 | Политика управления доступом | *Средства реализации*<br>Должна быть сформулирована, документирована и пересматриваться с точки зрения требований бизнеса и информационной безопасности политика управления доступом. |
| A.9.1.2 | Доступ к сетям и сетевым службам | *Средства реализации*<br>Пользователи должны получать доступ только к тем сетям и сетевым службам, для которых у них имеется авторизация. |
| **A.9.2 Управление доступом пользователей** | | |
| Задача: гарантировать доступ только авторизованных пользователей и предотвратить несанкционированный доступ к системам и услугам. | | |
| A.9.2.1 | Регистрация пользователей и отмена регистрации | *Средства реализации*<br>Должен быть внедрен надлежащим образом оформленный процесс регистрации и отмены регистрации пользователей, обеспечивающий возможность назначения прав доступа. |
| A.9.2.2 | Предоставление доступа пользователям | *Средства реализации*<br>Должен быть внедрен надлежащим образом оформленный процесс предоставления доступа пользователям для назначения или отмены прав всем типам пользователей ко всем системам и услугам. |
| A.9.2.3 | Управление привилегированными правами доступа | *Средства реализации*<br>Назначение и использование привилегированных прав доступа должно быть ограниченным и управляемым. |
| A.9.2.4 | Управление секретной информацией для аутентификации пользователей | *Средства реализации*<br>Формирование секретной информации для аутентификации пользователей должно быть управляемым посредством надлежащим образом оформленного процесса. |
| A.9.2.5 | Пересмотр пользовательских прав доступа | *Средства реализации*<br>Владельцы активов должны пересматривать права доступа пользователей через определенные интервалы времени. |
| A.9.2.6 | Удаление или изменение прав доступа | *Средства реализации*<br>Права доступа всех сотрудников и сторонних исполнителей к информации и устройствам обработки информации должны удаляться по окончании действия |

| | | |
|---|---|---|
| | | трудовых соглашений или настраиваться заново в соответствии с произошедшими изменениями. |
| **A.9.3 Обязанности пользователя** | | |
| Задача: сделать пользователей ответственными за сохранение их информации для аутентификации. | | |
| A.9.3.1 | Использование секретной информации для аутентификации | *Средства реализации*<br>Пользователям должно быть установлено требование следовать правилам организации в использовании секретной информации для аутентификации. |
| **A. 9.4 Управление доступом к системе и приложениям** | | |
| Задача: предотвратить несанкционированный доступ к системам и приложениям. | | |
| A.9.4.1 | Ограничение доступа к информации | *Средства реализации*<br>Доступ к информации и функциям прикладных систем должен быть ограничен в соответствии с политикой управления доступом. |
| A.9.4.2 | Безопасные процедуры входа в систему | *Средства реализации*<br>Там, где это требуется политикой управления доступом, доступ к системам и приложениям должен осуществляться в соответствии с безопасной процедурой входа в систему. |
| A.9.4.3 | Система управления паролями | *Средства реализации*<br>Системы управления паролями должны быть диалоговыми и гарантировать качественные пароли. |
| A.9.4.4 | Использование привилегированных утилит | *Средства реализации*<br>Применение утилит, которые могли бы обходить средства контроля системы и приложений, должно быть ограничено и жестко контролироваться. |
| A.9.4.5 | Управление доступом к исходному коду | *Средства реализации*<br>Доступ к исходному коду программ должен быть ограничен. |
| **A.10 Криптография** | | |
| **A.10.1 Криптографические методы** | | |
| Задача: гарантировать правильное и результативное использование криптографии для защиты конфиденциальности, подлинность и/или целостность информации. | | |
| A.10.1.1 | Политика по использованию криптографических методов | *Средства реализации*<br>Должна быть разработана и внедрена политика применения криптографических методов для защиты информации. |
| A.10.1.2 | Управление криптографическими | *Средства реализации*<br>Политика использования, защиты и срока действия |

| | | |
|---|---|---|
| | ключами | криптографических ключей к шифру должна быть разработана и применяться в течение всего жизненного цикла ключа. |
| **A.11 Физическая безопасность и защита от природных угроз** | | |
| **A.11.1 Охраняемая территория** | | |
| Задача: предотвратить несанкционированный физический доступ, повреждение и воздействие на информацию и средства для обработки информации организации. | | |
| A.11.1.1 | Физический периметр безопасности | *Средства реализации*<br>Периметры безопасности должны быть определены и использоваться для защиты мест нахождения ценной или особо важной информации и средств для обработки информации. |
| A.11.1.2 | Физические средства контроля за проходом | *Средства реализации*<br>Охраняемые территории должны быть защищены соответствующими средствами контроля прохода с целью гарантировать, что только имеющему права персоналу разрешен доступ. |
| A.11.1.3 | Безопасность офисов, помещений и устройств | *Средства реализации*<br>Меры обеспечения физической безопасности для офисов, помещений и устройств должны быть разработаны и применяться. |
| A.11.1.4 | Защита от внешних и природных угроз | *Средства реализации*<br>Меры обеспечения физической защиты от стихийных бедствий, злонамеренных нападений или аварий должны быть разработаны и применяться. |
| A.11.1.5 | Работа на охраняемой территории | *Средства реализации*<br>Процедуры работы на охраняемой территории должны быть разработаны и применяться. |
| A.11.1.6 | Площадки погрузки-разгрузки | *Средства реализации*<br>Места доступа, такие как площадки погрузки-разгрузки и прочие подобные им, где есть возможность пройти в помещение лицам без соответствующих прав, должны контролироваться и, если возможно, быть изолированными от средств обработки информации, чтобы избежать несанкционированного доступа. |
| **A.11.2 Оборудование** | | |
| Задача: предотвратить потерю, повреждение, кражу или компрометацию активов и нарушение деятельности организации. | | |
| A.11.2.1 | Расположение оборудования и защита | *Средства реализации*<br>Оборудование должно быть расположено и защищено так, чтобы уменьшить риск от природных угроз и |

| | | |
|---|---|---|
| | | вредных факторов, и возможности несанкционированного доступа. |
| A.11.2.2 | Службы обеспечения | *Средства реализации*<br>Оборудование должно быть защищены от перебоев в питании и других нарушений, вызванных перебоями в работе служб обеспечения. |
| A.11.2.3 | Безопасность кабельного хозяйства | *Средства реализации*<br>Питающие кабели и кабели, передающие данные или обеспечивающие работу информационных сервисов, должны быть защищены от перехвата, помех или повреждения. |
| A.11.2.4 | Обслуживание оборудования | *Средства реализации*<br>Оборудование должно надлежащим образом обслуживаться, чтобы гарантировать его постоянную доступность и исправность. |
| A.11.2.5 | Вынос активов | *Средства реализации*<br>Оборудование, информация или программное обеспечение не должны быть выноситься за пределы территории без предварительного разрешения. |
| A.11.2.6 | Безопасность оборудования и активов вне территории | *Средства реализации*<br>Меры обеспечения безопасности должны применяться к активам вне территории, принимая во внимание различные риски работы вне помещения организации. |
| A.11.2.7 | Безопасное списание или повторное использование оборудования | *Средства реализации*<br>Все единицы оборудования, содержащие носители данных, должны быть проверены, чтобы гарантировать, что любые ценные данные и имеющее лицензию программное обеспечение удалены или надлежащим образом переписаны до списания или повторного использования. |
| A.11.2.8 | Оставленное без присмотра пользовательское оборудование | *Средства реализации*<br>Пользователи должны гарантировать, что у оставленного без присмотра оборудования имеется соответствующая защита. |
| A.11.2.9 | Политика чистого стола и чистого экрана | *Средства реализации*<br>Должна быть установлена политика чистого стола для бумажных документов и сменных носителей информации, и политика чистого экрана для средств для обработки информации. |

| | | |
|---|---|---|
| **A.12 Безопасность в период эксплуатации** | | |
| **A.12.1 Эксплуатационные процедуры и обязанности** | | |
| Задача: гарантировать надлежащую и безопасную эксплуатацию средств обработки информации. | | |
| A.12.1.1 | Документированные рабочие процедуры | *Средства реализации*<br>Рабочие процедуры должны быть документированы и доступны всем пользователям, которым они необходимы. |
| A.12.1.2 | Управление изменениями | *Средства реализации*<br>Изменения в организации, бизнес-процессах, средствах для обработки информации и системах, которые влияют на информационную безопасность, должны быть управляемыми. |
| A.12.1.3 | Управление производительностью | *Средства реализации*<br>Применяемые ресурсы должны быть настроены, должен вестись мониторинг их использования и оценка требуемой в перспективе их производительности должна гарантировать необходимую работоспособность системы. |
| A.12.1.4 | Разделение среды разработки, тестирования и эксплуатации | *Средства реализации*<br>Среда разработки, среда тестирования и среда эксплуатации должны быть отделены друг от друга, чтобы снизить риски несанкционированного доступа или изменений в операционной среде. |
| **A.12.2 Защита от вредоносного кода** | | |
| Задача: гарантировать, что информация и средства обработки информации защищены от вредоносного кода. | | |
| A.12.2.1 | Средства защиты от вредоносного кода | *Средства реализации*<br>В отношении вредоносного кода должны применяться меры по обнаружению, предупреждению и восстановлению, сопровождаемые соответствующим информированием пользователей. |
| **A.12.3 Резервное копирование** | | |
| Задача: защитить данные от потери. | | |
| A.12.3.1 | Резервное копирование информации | *Средства реализации*<br>Должно выполняться и регулярно тестироваться резервное копирование информации, программного обеспечения и образа системы в соответствии с принятой политикой резервного копирования. |

| | | |
|---|---|---|
| **A.12.4 Регистрация и мониторинг** | | |
| Задача: фиксировать события, чтобы обеспечивать доказательства. | | |
| A.12.4.1 | Регистрация событий | *Средства реализации*<br>Должен вестись, сохраняться и регулярно просматриваться журнал (лог), содержащий записи активности пользователей, возникновения исключений, сбоев и событий, связанных с информационной безопасностью. |
| A.12.4.2 | Защита регистрационной информации (логов) | *Средства реализации*<br>Средства для ведения записей (логов) и внесенная в них информация должны быть защищены от вмешательства и несанкционированного доступа. |
| A.12.4.3 | Регистрация действий администраторов и операторов | *Средства реализации*<br>Должны быть зарегистрированы действия системных администраторов и операторов, логи должны быть защищены и регулярно просматриваться. |
| A.12.4.4 | Синхронизация часов | *Средства реализации*<br>Время у всех информационных систем, обрабатывающих важную информацию, в пределах организации или домена безопасности должно быть синхронизировано с единым эталоном времени. |
| **A.12.5 Управление используемым программным обеспечением** | | |
| Задача: гарантировать целостность эксплуатируемых систем. | | |
| A.12.5.1 | Установка программного обеспечения в эксплуатируемых системах | *Средства реализации*<br>Должны быть внедрены процедуры для управления установкой программного обеспечения в эксплуатируемых системах. |
| **A.12.6 Управление технической уязвимостью** | | |
| Задача: предотвратить использование технических уязвимостей. | | |
| A.12.6.1 | Контроль технических уязвимостей | *Средства реализации*<br>Должна получаться своевременно информация о технических уязвимостях используемых информационных систем, должны оцениваться риски организации от таких уязвимостей и приниматься соответствующие меры для обработки этих рисков. |
| A.12.6.2 | Ограничения на установку программного обеспечения | *Средства реализации*<br>Правила, регулирующие установку программного обеспечения пользователями, должны быть разработаны и внедрены. |

| | | |
|---|---|---|
| **A.12.7 Ограничения, связанные с аудитом информационных систем** | | |
| Задача: минимизировать воздействие аудита на эксплуатируемые системы. | | |
| A.12.7.1 | Управление аудитом информационных систем | *Средства реализации*<br>Требования и действия по аудиту, направленному на проверку эксплуатируемых систем, должны тщательно планироваться и согласовываться с целью минимизации нарушений нормального выполнения бизнес-процессов. |
| **A.13 Сетевая безопасность** | | |
| **A.13.1 Управление сетевой безопасностью** | | |
| Задача: гарантировать защиту информации в сетях и поддерживающих сети средств обработки информации. | | |
| A.13.1.1 | Управление сетями | *Средства реализации*<br>Сети должны управляться и контролироваться, чтобы защитить информацию в системах и приложениях. |
| A.13.1.2 | Безопасность сетевого обслуживания | *Средства реализации*<br>Должны быть определены для всех услуг и включены в соглашения по обслуживанию сетей механизмы обеспечения безопасности, уровни сервиса и требования к управлению, осуществляются ли эти услуги внутренними подразделениями или сторонней организацией. |
| A.13.1.3 | Разделение в сетях | *Средства реализации*<br>Различные группы информационных служб, пользователей и информационных систем должны быть разделены в сетях. |
| **A.13.2 Передача информации** | | |
| Задача: обеспечить безопасность информации, передаваемой внутри организации и за ее пределы. | | |
| A.13.2.1 | Политика и процедуры передачи информации | *Средства реализации*<br>На местах должны быть установленные политики передачи информации, процедуры и средства управления с целью защиты информации, передаваемой любыми типами коммуникационного оборудования. |
| A.13.2.2 | Соглашения по передаче информации | *Средства реализации*<br>Соглашения должны регламентировать безопасную передачу бизнес-информации между организацией и внешними сторонами. |
| A.13.2.3 | Передача электронных сообщений | *Средства реализации*<br>Информация, передаваемая электронными сообщениями, должна быть соответственным образом защищена. |

| | | |
|---|---|---|
| A.13.2.4 | Соглашения о конфиденциальности или неразглашении | *Средства реализации*<br>Требования к соглашениям о конфиденциальности или неразглашении, отражающие потребности организации в защите информации, должны быть определены, документированы и регулярно пересматриваться. |
| **A.14 Приобретение, разработка и обслуживание систем** | | |
| **A.14.1 Требования по безопасности информационных систем** | | |
| Задача: гарантировать, что информационная безопасность является неотъемлемой частью информационных систем в течение всего их жизненного цикла. Это также относится и к требованиям для информационных систем, которые предоставляют сервисы в общедоступных сетях. | | |
| A.14.1.1 | Анализ и спецификация требований по информационной безопасности | *Средства реализации*<br>Требования, связанные с информационной безопасностью должны быть включены в требования для новых информационных систем или расширения к существующим информационным системам. |
| A.14.1.2 | Безопасность прикладных сервисов в общедоступных сетях | *Средства реализации*<br>Информация, обрабатываемая прикладными сервисами, передающими информацию по общедоступным сетям, должна быть защищена от мошеннических действий, несанкционированного раскрытия и изменения и не вызывать юридических споров. |
| A.14.1.3 | Защита транзакций прикладных сервисов | *Средства реализации*<br>Информация, обрабатываемая в ходе транзакций, осуществляемых прикладными сервисами, должна быть защищена с целью предотвращения незавершенной передачи, неправильной маршрутизации, несанкционированного изменения сообщения, несанкционированного раскрытия, несанкционированного дублирования сообщения или воспроизведения. |
| **A.14.2 Безопасность в процессах разработки и поддержки** | | |
| Задача: гарантировать, что меры по обеспечению информационной безопасности разработаны и реализуются в течение всего цикла разработки информационных систем. | | |
| A.14.2.1 | Политика разработки | *Средства реализации*<br>Правила для разработки программного обеспечения и систем должны быть установлены и применяться ко всем разработкам в организации. |
| A.14.2.2 | Процедуры управления изменениями | *Средства реализации*<br>Изменения в системах в течение цикла разработки должны быть управляемыми посредством надлежащим образом установленных процедур управления |

| | | |
|---|---|---|
| | | изменениями. |
| A.14.2.3 | Анализ приложений после изменений в операционной платформе | *Средства реализации*<br>После смены операционных платформ, наиболее критичные бизнес-приложения должны быть проанализированы и протестированы, чтобы гарантировать, что отсутствует негативное влияние на деятельность организации или безопасность. |
| A.14.2.4 | Ограничения на изменения пакетов программ | *Средства реализации*<br>Модификация пакетов программ не должна поощряться и должна быть ограничена только необходимыми изменениями, а все изменения должны строго контролироваться. |
| A.14.2.5 | Принципы разработки безопасных систем | *Средства реализации*<br>Принципы разработки безопасных систем должны быть установлены, документированы, поддерживаться и применяться во всех случаях внедрения информационных систем. |
| A.14.2.6 | Безопасная среда разработки | *Средства реализации*<br>Организации должны устанавливать и соответствующим образом защищать безопасную среду проектирования для работ по разработке и интеграции систем, охватывающих весь цикл проектирования систем. |
| A.14.2.7 | Разработка на аутсорсинге | *Средства реализации*<br>Организация должна контролировать и вести мониторинг процесса разработки системы, переданного на аутсорсинг. |
| A.14.2.8 | Тестирование безопасности системы | *Средства реализации*<br>В ходе разработки должно выполняться тестирование функциональности, связанной с безопасностью. |
| A.14.2.9 | Приемочное тестирование системы | *Средства реализации*<br>Должно быть выбрано тестовое программное обеспечение и установлены критерии приемки для новых информационных систем, обновлений и новых версий. |
| **A.14.3 Данные для тестирования** | | |
| Задача: обеспечить защиту данных, используемых для тестирования. | | |
| A.14.3.1 | Защита данных для тестирования | *Средства реализации*<br>Данные для тестирования должны тщательно выбираться, быть защищенными и контролироваться. |

| | | |
|---|---|---|
| **A.15 Отношения с поставщиками** | | |
| **A.15.1 информационная безопасность в отношениях с поставщиками** | | |
| Задача: гарантировать защиту активов организации, которые доступны поставщикам. | | |
| A.15.1.1 | Политика информационной безопасности в отношениях с поставщиками | *Средства реализации*<br>Требования по информационной безопасности для снижения рисков, связанных с доступом поставщиков к активам организации, должны быть согласованы с поставщиками и документированы. |
| A.15.1.2 | Поддержка безопасности в рамках соглашений с поставщиками | *Средства реализации*<br>Все существенные требования по информационной безопасности должны быть установлены и согласованы с каждым поставщиком, который может получать доступ, обрабатывать, хранить, передавать информацию организации или поставлять компоненты для ИТ-инфраструктуры. |
| A.15.1.3 | Цепочка поставок для информационно-коммуникационных технологий | *Средства реализации*<br>Соглашения с поставщиками должны включать требования, учитывающие риски информационной безопасности, связанные с услугами в сфере информационно-коммуникационных технологий и системой поставок продукции. |
| **A.15.2 Управление предоставлением услуг поставщиком** | | |
| Задача: поддерживать согласованный уровень информационной безопасности и предоставления услуг в соответствии с соглашениями с поставщиком. | | |
| A.15.2.1 | Контроль и анализ услуг поставщика | *Средства реализации*<br>Организации должны регулярно контролировать, анализировать и проводить аудит предоставления услуг поставщиком. |
| A.15.2.2 | Управление изменениями услуг поставщика | *Средства реализации*<br>Изменения в предоставлении услуг поставщиками, включая поддержание и улучшение существующих политик информационной безопасности, процедур и средств управления, должны управляться, с учетом критичности бизнес-информации, используемых систем и процессов и повторной оценки рисков. |
| **A.16 Управление инцидентами в сфере информационной безопасности** | | |
| **A.16.1 Управление инцидентами информационной безопасности и улучшения** | | |
| Задача: гарантировать последовательный и результативный подход к управлению инцидентами информационной безопасности, включая информирование о событиях, связанных с безопасностью, и уязвимостях. | | |
| A.16.1.1 | Ответственность и | *Средства реализации* |

| | | |
|---|---|---|
| | процедуры | Должна быть установлена ответственность и процедуры, чтобы гарантировать быстрый, результативный и надлежащий ответ на инциденты информационной безопасности. |
| A.16.1.2 | Сообщение о событиях информационной безопасности | *Средства реализации*<br>Информация о событиях, связанных с безопасностью, должна доводиться до руководства через соответствующие каналы как можно быстрее. |
| A.16.1.3 | Сообщение об уязвимостях в информационной безопасности | *Средства реализации*<br>От сотрудников и работающих по контракту, использующих информационные системы и сервисы организации, необходимо требовать фиксировать и докладывать о любых обнаруженных или предполагаемых уязвимостях в информационной безопасности систем и сервисов. |
| A.16.1.4 | Оценка и решение по событию информационной безопасности | *Средства реализации*<br>События, связанные с информационной безопасностью, должны оцениваться и затем приниматься решение, следует ли их классифицировать как инцидент информационной безопасности. |
| A.16.1.5 | Ответ на инцидент информационной безопасности | *Средства реализации*<br>Реагирование на инциденты информационной безопасности должно осуществляться в соответствии с документированными процедурами. |
| A.16.1.6 | Учет опыта инцидентов информационной безопасности | *Средства реализации*<br>Знания, полученные из анализа и разрешения инцидентов информационной безопасности, должны использоваться для уменьшения вероятности инцидентов в будущем или их воздействия. |
| A.16.1.7 | Сбор свидетельств | *Средства реализации*<br>Организация должна определить и применять процедуры для идентификации, сбора, получения и сохранения информации, которая может служить в качестве свидетельств. |
| **A.17 Аспекты информационной безопасности управления непрерывностью бизнеса** | | |
| **A.17.1 Непрерывность информационной безопасности** | | |
| Задача: Непрерывность информационной безопасности должна быть неотъемлемым результатом работы системы управления непрерывностью бизнеса организации. | | |
| A.17.1.1 | Планирование непрерывности информационной безопасности | *Средства реализации*<br>Организация должна определить свои требования к информационной безопасности и управлению непрерывностью информационной безопасности в |

| | | |
|---|---|---|
| | | неблагоприятных ситуациях, например, во время кризиса или стихийного бедствия. |
| A.17.1.2 | Осуществление непрерывности информационной безопасности | *Средства реализации*<br>Организация должна установить, документировать, внедрить и поддерживать процессы, процедуры и средства управления, чтобы гарантировать необходимый уровень непрерывности информационной безопасности во время неблагоприятной ситуации. |
| A.17.1.3 | Проверка, анализ и оценка непрерывности информационной безопасности | *Средства реализации*<br>Организация должна проверять установленные и внедренные средства управления непрерывностью информационной безопасности через определенные интервалы времени, чтобы гарантировать, что эти средства пригодны и результативны во время неблагоприятных ситуаций. |
| **A.17.2 Резервирование** | | |
| Задача: гарантировать доступность средств обработки информации. | | |
| A.17.2.1 | Доступность средств обработки информации | *Средства реализации*<br>Средства обработки информации должны резервироваться с избыточностью, достаточной для обеспечения требований по доступности. |
| **A.18 Соответствие** | | |
| **A.18.1 Соответствие законодательным и договорными требованиям** | | |
| Задача: избегать нарушений законодательных, нормативных и иных обязательных требований или договорных обязательств, имеющих отношение к информационной безопасности, а также любых требований по безопасности. | | |
| A.18.1.1 | Определение применимых законодательных и договорных требований | *Средства реализации*<br>Все существенные законодательные, нормативные, иные обязательные, договорные требования, а также подход организации к удовлетворению этих требований должны быть явным образом определены, документированы и сохраняться актуальными для каждой информационной системы и организации. |
| A.18.1.2 | Права интеллектуальной собственности | *Средства реализации*<br>Соответствующие процедуры должны быть внедрены, чтобы гарантировать соответствие законодательным, нормативным и договорным требованиям, связанным с правами на интеллектуальную собственность и использованием программных продуктов, являющихся чей-то собственностью. |
| A.18.1.3 | Защита записей | *Средства реализации*<br>Записи должны быть защищены от потери, повреждения, |

| | | |
|---|---|---|
| | | фальсификации, несанкционированного доступа и несанкционированного выпуска в соответствии с законодательными, нормативными, договорными требованиями и требованиями бизнеса. |
| A.18.1.4 | Конфиденциальность и защита персональных данных | *Средства реализации*<br>Конфиденциальность и защита персональных данных должны быть обеспечены в той мере, в какой это требуется соответствующим законодательством и применимыми нормативными актами. |
| A.18.1.5 | Регулирование криптографических методов | *Средства реализации*<br>Криптографические методы должны использоваться в соответствии со всеми применимыми соглашениями, требованиями законодательства и нормативных актов. |
| **A.18.2 Анализ информационной безопасности** | | |
| Задача: гарантировать, что информационная безопасность обеспечивается и управляется в соответствии с организационной политикой и процедурами. | | |
| A.18.2.1 | Независимый анализ информационной безопасности | *Средства реализации*<br>Подход организации к управлению информационной безопасностью и его реализация (т. е. целевые задачи, средства управления, политики, процессы и процедуры по информационной безопасности) должны анализироваться независимым образом в запланированные интервалы времени или в тех случаях, когда происходят существенные изменения. |
| A.18.2.2 | Соответствие политикам безопасности и стандартам | *Средства реализации*<br>Руководители в пределах своей области ответственности должны регулярно анализировать на соответствие политикам безопасности, стандартам и любым другими требованиям по безопасности процессы обработки информации и процедуры. |
| A.18.2.3 | Анализ технического соответствия | *Средства реализации*<br>Информационные системы должны регулярно анализироваться на предмет соответствия политикам информационной безопасности организации и стандартам. |

# Библиография

[1] ISO/IEC 27002:2013, Information technology — Security Techniques — Code of practice for information security controls

[2] ISO/IEC 27003, Information technology — Security techniques — Information security management system implementation guidance

[3] ISO/IEC 27004, Information technology — Security techniques — Information security management — Measurement

[4] ISO/IEC 27005, Information technology — Security techniques — Information security risk management

[5] ISO 31000:2009, Risk management — Principles and guidelines

[6] ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, 2012