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 обеспечивает сохранение конфиденциальности, целостности и возможности применения информации за счет выполнения процесса менеджмента риска и дает уверенность заинтересованным сторонам 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 управлять 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 действия системы менеджмента информационной безопасности

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

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

b) гарантии того, что требования системы менеджмента информационной безопасности встроены в процессы организации;

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

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

e) гарантии 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) поощрения демонстрации лидерства на различных уровнях управления в границах

установленной ответственности.

5.2 Политика

Высшее руководство должно установить политику информационной безопасности, которая:

a) соответствует назначению организации;

b) включает цели (задачи) в области информационной безопасности, (см. раздел 6.2) или служит основой для задания таких целей (задач);

c) включает обязательство соответствовать действующим требованиям, связанным 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 доведена до сведения сотрудников 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 по обработке рисков и реализации 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 по обработке этих рисков и реализации возможностей; и

e) каким образом

1) встраивать эти действия в процессы системы менеджмента информационной безопасности и выполнять 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 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 возможности применения информации в рамках области действия 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 величины 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 упущены из виду;

ПРИМЕЧАНИЕ 1 Приложение А содержит полный перечень задач управления и соответствующих средств для их реализации. Пользователи Настоящего Международного Стандарта обязаны использовать Приложение А с тем, чтобы гарантировать, что никакие необходимые средства управления не были пропущены.

ПРИМЕЧАНИЕ 2 Задачи управления неявным образом включены в выбранные средства управления. Задачи управления и средства их реализации, 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));
- обоснование их применения;
- применяются ли эти средства управления в данный момент или нет; а также
- обоснование исключения любых 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 Цели в области информационной безопасности и планирование их достижения

Организация должна установить цели в области информационной безопасности для соответствующих функций и уровней.

Цели в области информационной безопасности должны:

a) быть согласованными с политикой информационной безопасности;

b) быть измеримыми (если возможно);

c) учитывать действующие 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 целям в области информационной безопасности как документированную информацию.

При планировании, каким образом достигнуть своих целей в области информационной безопасности, организация должна определить:

f) что будет сделано;

g) какие ресурсы потребуются;

h) кто будет ответственным;

i) когда цели будут достигнуты; и

j) как результаты будут оцениваться.

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 контролем 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 либо привлечение по контракту компетентных специалистов.

7.3 Осведомленность

Персонал, выполняющий работу под контролем 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 должны осуществляться коммуникации.

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 и услуг,

2) сложности процессов и их взаимодействий 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 там, 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 читаемости,

c) управлять изменениями (например, контроль версий), и

d) устанавливать срок хранения и методы уничтожения.

Документированная информация внешнего происхождения, признанная организацией необходимой для планирования и функционирования системы менеджмента информационной безопасности, 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 Оперативное планирование и управление

Организация должна планировать, осуществлять и управлять процессами, необходимыми для обеспечения соответствия требованиям информационной безопасности, и выполнять действия, определенные в п. 6.1. Организация должна также выполнять запланированные

действия для достижения целей, 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 функционирование 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 информационной безопасности результативно внедрена и функционирует.

Организация должна:

c) планировать, разрабатывать, 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 соответствующим руководителям, и

g) сохранять документированную информацию как подтверждение программы аудита и его результатов.

9.3 Анализ менеджмента

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

При анализе менеджмента необходимо учитывать следующее:

a) статус мероприятий, предусмотренных предыдущим анализом;

b) изменения в состоянии внешних и внутренних проблем, которые существенны для системы менеджмента информационной безопасности;

c) информацию 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 целей в области информационной безопасности;

d) обратную связь от заинтересованных сторон;

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

f) 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 сохранять документированную информацию как подтверждение результатов анализа системы менеджмента.

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 документированную информацию как свидетельство:

f) характера несоответствий и любых последующих предпринятых действий; и
g) результатов любого корректирующего действия.

10.2 Непрерывное улучшение

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

Приложение А
(нормативное)
Связь целей (задач) управления и средств их реализации

Цели (задачи) управления 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 – Цели (задачи) и средства их реализации

А.5 Политики информационной безопасности		
А.5.1 Ориентация менеджмента на информационную безопасность		
Задача: обеспечить ориентацию менеджмента и поддержку информационной безопасности в соответствии с требованиями бизнеса и соответствующими законодательными и нормативными требованиями.		
А5.1.1.	Политики информационной безопасности	*Средства реализации* Должен быть разработан, одобрен руководством, опубликован и доведен до персонала и соответствующих внешних сторон комплекс политик информационной безопасности.
А.5.1.2	Пересмотр политик информационной безопасности	*Средства реализации* Политики информационной безопасности для гарантии их постоянной пригодности, соответствия и результативности должны пересматриваться через запланированные интервалы времени или в случае существенных изменений.
А.6 Организация информационной безопасности		
А.6.1 Внутренняя организация		
Задача: сформировать основные элементы управления для инициирования и контроля внедрения и эксплуатации средств защиты информации в организации.		
А.6.1.1	Должностные функции и обязанности, связанные с информационной безопасностью	*Средства реализации* Должны быть определены и назначены все обязанности, связанные с информационной безопасностью.
А.6.1.2	Разделение обязанностей	*Средства реализации* Вступающие в противоречие друг с другом обязанности и области ответственности должны быть разделены для снижения возможности несанкционированного или ненамеренного изменения или неправильного применения активов организации.

A.6.1.3	Контакты с полномочными органами	*Средства реализации* Должны поддерживаться соответствующие контакты с полномочными органами.
A.6.1.4	Контакты с профессиональными сообществами	*Средства реализации* Должны поддерживаться соответствующие контакты с профессиональными сообществами или иными форумами специалистов по информационной безопасности и профессиональными ассоциациями.
A.6.1.5	Информационная безопасность в управлении проектами	*Средства реализации* Вопросы информационной безопасности должны приниматься во внимание в управлении проектами вне зависимости 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* Должны быть приняты политика и меры по обеспечению безопасности для управления рисками, связанными с использованием мобильных устройств.
A.6.2.2	Удаленная работа	*Средства реализации* Должны быть приняты политика и меры обеспечения безопасности для защиты информации, к которой осуществляется доступ на удаленных рабочих местах и которая там обрабатывается или сохраняется.
A.7 Безопасность персонала		
A.7.1 До приема на работу		
Задача: гарантировать, что сотрудники и привлекаемые по контракту понимают свои обязанности и соответствуют тем должностным функциям, которые им предполагается поручить.		
A.7.1.1	Предварительная проверка	*Средства реализации* Проверка при приеме на работу, осуществляемая для всех кандидатов, должна проводиться в рамках соответствующих законодательных актов, регламентов и этических норм, а также должна быть соразмерна бизнес-требованиям, категории информации по классификации, к которой предполагается доступ, и предполагаемым рискам.
A.7.1.2	Условия трудового соглашения	*Средства реализации* Трудовые соглашения с сотрудниками или привлекаемыми по контракту должны устанавливать их и организации ответственность в части информационной безопасности.

A.7.2 В период занятости		
Задача: гарантировать, что сотрудники и работающие по контракту знают и выполняют свои обязательства, связанные с информационной безопасностью.		
A.7.2.1	Ответственность руководства	*Средства реализации* 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	Осведомленность, образование и обучение в сфере информационной безопасности	*Средства реализации* Все сотрудники организации и, там, где это существенно, работающие по контракту должны быть соответствующим образом информированы и обучены, а также регулярно извещаться об изменениях в политиках и процедурах организации, в той мере, насколько это важно для исполнения их служебных обязанностей.
A.7.2.3	Дисциплинарные меры	*Средства реализации* Должен быть разработан и доведен до сведения персонала процесс для принятия мер к тем сотрудникам, которые допустили нарушение требований информационной безопасности.
A.7.3 Прекращение и изменение трудовых отношений		
Задача: защитить интересы организации при изменении обязанностей сотрудника или прекращении с ним трудовых отношений.		
A.7.3.1	Освобождение от обязанностей или их изменение	*Средства реализации* Должны быть определены, доведены до сведения сотрудника или работающего по контракту его область ответственности и обеспечено выполнение его обязанностей в отношении информационной безопасности, остающихся в силе после прекращения или изменения трудовых отношений.
A.8 Управление активами		
A.8.1 Ответственность за активы		
Задача: выявить активы организации и определить соответствующую ответственность по их защите.		
A.8.1.1	Инвентаризация активов	*Средства реализации* Информация, другие активы, связанные с информацией и устройствами обработки информации, должны быть выявлены и составлен реестр этих активов, который должен поддерживаться в актуальном состоянии.

A.8.1.2	Владение активами	*Средства реализации* У активов, включенных в реестр, должны быть владельцы.
A.8.1.3	Надлежащее использование активов	*Средства реализации* 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* Все сотрудники и внешние пользователи должны вернуть все активы организации в ее распоряжение по окончании действия трудовых договоров, контрактов и 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* Информация должна быть классифицирована с точки зрения юридических требований, содержания, критичности и уязвимости для несанкционированного раскрытия и изменения.
A.8.2.2	Маркировка информации	*Средства реализации* Должен быть разработан и внедрен соответствующий набор процедур для маркировки информации в соответствии со схемой классификации информации, принятой в организации.
A.8.2.3	Обращение с активами	*Средства реализации* Должны быть разработаны и внедрены процедуры обращения с активами в соответствии со схемой классификации информации, принятой в организации.
A.8.3 Обращение с носителями информации		
Задача: предотвратить несанкционированное раскрытие, изменение, перемещение или уничтожение информации, хранимой на носителе.		
A.8.3.1	Управление съемными носителями	*Средства реализации* Должны быть внедрены процедуры для управления съемными носителями в соответствии со схемой классификации, принятой в организации.
A.8.3.2	Утилизация носителей информации	*Средства реализации* Носители, если в них больше нет необходимости, должны быть утилизированы надежным способом в соответствии с установленными процедурами.

A.8.3.3	Физическое перемещение носителей информации	*Средства реализации* Носители информации во время транспортировки должны быть защищены от несанкционированного доступа, нецелевого использования или повреждения.
A.9 Контроль доступа		
A.9.1 Диктуемые бизнесом требования к контролю доступа		
Задача: ограничить доступ к информации и устройствам ее обработки.		
A.9.1.1	Политика контроля доступа	*Средства реализации* Политика контроля доступа должна быть сформулирована, документирована и пересматриваться с точки зрения требований бизнеса и информационной безопасности.
A.9.1.2	Доступ к сетям и сетевым службам	*Средства реализации* Пользователи должны получать доступ только к тем сетям и сетевым службам, для которых у них есть авторизация.
A.9.2 Управление доступом пользователей		
Задача: гарантировать авторизованный доступ пользователя и предотвратить несанкционированный доступ к системам и службам.		
A.9.2.1	Регистрация и отмена регистрации пользователя	*Средства реализации* Должен быть внедрен формализованный процесс регистрации и отмены регистрации пользователей, обеспечивающий возможность назначения прав доступа.
A.9.2.2	Предоставление доступа пользователю	*Средства реализации* Должен быть внедрен формализованный 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* Назначение и использование привилегированных прав доступа должно быть ограниченным и контролируемым.
A.9.2.4	Управление секретной информацией аутентификации пользователей	*Средства реализации* Присваивание секретной информации аутентификации должно быть контролируемым через формализованный процесс управления.
A.9.2.5	Пересмотр прав доступа пользователей	*Средства реализации* Владельцы активов должны пересматривать права доступа пользователей через регулярные промежутки времени.

A.9.2.6	Отмена или изменение прав доступа	*Средства реализации* Права доступа к информации и устройствам обработки информации всех сотрудников и внешних пользователей должны быть отменены после завершения трудовых отношений, контракта или соглашения.
A.9.3 Обязанности пользователей		
Задача: сделать пользователей ответственными за сохранение их информации аутентификации.		
A.9.3.1	Использование секретной информации аутентификации	*Средства реализации* Пользователи обязаны следовать правилам организации при использовании секретной аутентификационной информации.
A. 9.4 Контроль доступа к системе и приложениям		
Задача: предотвратить несанкционированный доступ к системам и приложениям.		
A.9.4.1	Ограничение доступа к информации	*Средства реализации* Доступ к информации и функциям прикладных систем должен быть ограничен в соответствии с политикой контроля доступа.
A.9.4.2	Безопасные процедуры входа в систему	*Средства реализации* Там, где это требуется политикой контроля доступа, доступ к системам и приложениям должен осуществляться в соответствии с безопасной процедурой входа в систему.
A.9.4.3	Система управления паролями	*Средства реализации* Системы управления паролями должны быть диалоговыми и гарантировать пароли надлежащего качества.
A.9.4.4	Использование утилит с привилегированными правами	*Средства реализации* Применение утилит, которые могли бы обходить средства контроля системы и приложений, должно быть ограничено и жестко контролироваться.
A.9.4.5	Контроль доступа к исходным кодам	*Средства реализации* Доступ к исходному коду программ должен быть ограничен.
A.10 Криптография		
A.10.1 Криптографические методы защиты		
Задача: гарантировать надлежащее и результативное использование криптографии для защиты конфиденциальности, подлинности и/или целостности информации.		

A.10.1.1	Политика использования криптографических методов защиты	*Средства реализации* Должна быть разработана и внедрена политика использования криптографических методов для защиты информации.
A.10.1.2	Управление ключами	*Средства реализации* Политика использования, защиты и срока действия криптографических ключей должна быть разработана и применяться в течение всего жизненного цикла ключей.
A.11 Физическая безопасность и защита от природных угроз		
A.11.1 Охраняемая зона		
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* Периметры безопасности должны быть определены и использоваться для защиты зон нахождения уязвимой или особо важной информации и средств для обработки информации.
A.11.1.2	Средства контроля прохода	*Средства реализации* Охраняемые зоны должны быть защищены соответствующими средствами контроля прохода с целью гарантировать, что только имеющему права персоналу разрешен доступ.
A.11.1.3	Защита офисов, помещений и устройств	*Средства реализации* Меры защиты для офисов, помещений и оборудования должны быть разработаны и применяться.
A.11.1.4	Защита от внешних угроз и угроз природного характера	*Средства реализации* Должны быть разработаны и применяться меры физической защиты от стихийных бедствий, злонамеренных действий или аварий.
A.11.1.5	Работа в охраняемых зонах	*Средства реализации* Должны быть разработаны и применяться процедуры для работы в охраняемой зоне.
A.11.1.6	Зоны доставки и отгрузки	*Средства реализации* Места доступа, такие как зоны доставки и отгрузки и иные, где есть возможность пройти в помещение лицам без соответствующих прав, должны контролироваться и, если возможно, быть изолированными от средств обработки информации, чтобы избежать несанкционированного доступа.
A.11.2 Оборудование		

Задача: предотвратить потерю, повреждение, кражу или компрометацию активов и нарушение деятельности организации.		
A.11.2.1	Размещение и защита оборудования	*Средства реализации* Оборудование должно быть размещено и защищено так, чтобы снизить риски, связанные с природными угрозами и опасностями, а также возможностью несанкционированного доступа.
A.11.2.2	Службы обеспечения	*Средства реализации* Оборудование должно быть защищено от перебоев в электроснабжении и других нарушений, вызванных перебоями в работе служб обеспечения.
A.11.2.3	Защита кабельных сетей	*Средства реализации* 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* Оборудование должно надлежащим образом обслуживаться, чтобы гарантировать его постоянную готовность и исправность.
A.11.2.5	Вынос активов	*Средства реализации* Оборудование, информация или программное обеспечение не должны выноситься за пределы территории без предварительного разрешения.
A.11.2.6	Защита оборудования и активов вне территории	*Средства реализации* Меры обеспечения безопасности должны применяться к активам вне территории, принимая во внимание различные риски работы вне помещений организации.
A.11.2.7	Безопасная утилизация или повторное использование оборудования	*Средства реализации* Все элементы оборудования, содержащие накопители, должны быть проверены, чтобы гарантировать, что любые ценные данные и лицензионное программное обеспечение удалены или надежным образом затерты новой информацией до утилизации или повторного использования.
A.11.2.8	Оборудование пользователя, оставленное без присмотра	*Средства реализации* Пользователи должны гарантировать, что у оставленного без присмотра оборудования имеется соответствующая защита.

A.11.2.9	Политика чистого стола и чистого экрана	*Средства реализации* Должна быть установлена политика чистого стола для бумажных документов и сменных носителей информации, и политика чистого экрана для устройств обработки информации.
A.12 Безопасность производственной деятельности		
A.12.1 Рабочие процедуры и обязанности		
Задача: гарантировать надлежащую и безопасную эксплуатацию средств обработки информации.		
A.12.1.1	Документированные рабочие процедуры	*Средства реализации* Рабочие процедуры должны быть документированы и доступны всем пользователям, которым они необходимы.
A.12.1.2	Управление изменениями	*Средства реализации* 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* Использование ресурсов должно отслеживаться, регулироваться и делаться прогноз требований к производительности в будущем с тем, чтобы гарантировать необходимую работоспособность систем.
A.12.1.4	Разделение среды разработки, тестирования и эксплуатации	*Средства реализации* Среда разработки, тестирования и рабочая среда должны быть отделены друг от друга для снижения рисков 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	Меры защиты от вредоносного кода	*Средства реализации* В отношении вредоносного кода должны применяться меры по обнаружению, предупреждению и восстановлению с соответствующим информированием пользователей.
A.12.3 Резервное копирование		
Задача: обеспечить защиту от потери данных.		

A.12.3.1	Резервное копирование информации	*Средства реализации* Должно выполняться и регулярно тестироваться резервное копирование информации, программного обеспечения и образов системы в соответствии с принятой политикой резервного копирования.
A.12.4 Ведение журналов и мониторинг		
Задача: регистрировать события и обеспечивать свидетельства.		
A.12.4.1	Регистрация событий	*Средства реализации* Должен вестись, сохраняться и регулярно анализироваться журналы, содержащие записи активности пользователей, возникновения исключений, сбоев и событий, связанных с информационной безопасностью.
A.12.4.2	Защита информации в журналах	*Средства реализации* Средства для ведения журналов и внесенная в них информация должны быть защищены от несанкционированного вмешательства и несанкционированного доступа.
A.12.4.3	Журналы действий администратора и оператора	*Средства реализации* Должны быть зафиксированы действия системных администраторов и операторов, журналы должны быть защищены и регулярно просматриваться.
A.12.4.4	Синхронизация часов	*Средства реализации* Время у всех информационных систем, обрабатывающих важную информацию, в пределах организации или домена безопасности должно быть синхронизировано с единым источником эталонного времени.
A.12.5 Контроль эксплуатируемого программного обеспечения		
Задача: гарантировать целостность эксплуатируемых систем.		
A.12.5.1	Установка программ в эксплуатируемых системах	*Средства реализации* Должны быть внедрены процедуры для управления установкой программного обеспечения в эксплуатируемых системах.
A.12.6 Управление техническими уязвимостями		
Задача: предотвратить использование технических уязвимостей.		

A.12.6.1	Управление техническими уязвимостями	*Средства реализации* Должна своевременно получаться информация о технических уязвимостях в используемых информационных системах, должно оцениваться влияние этих уязвимостей на организацию и приниматься соответствующие меры для обработки связанных с этим рисков.
A.12.6.2	Ограничения на установку программного обеспечения	*Средства реализации* Правила, регулирующие установку программного обеспечения пользователями, должны быть разработаны и внедрены.
A.12.7 Ограничения на аудит информационных систем		
Задача: минимизировать воздействие аудита на эксплуатируемые системы.		
A.12.7.1	Средства управления аудитом информационных систем	*Средства реализации* 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 Безопасность обмена информацией		
A.13.1 Управление сетевой безопасностью		
Задача: гарантировать защиту информации в сетях и на поддерживающих их средствах обработки информации.		
A.13.1.1	Средства управления сетями	*Средства реализации* Сети должны управляться и контролироваться, чтобы защитить информацию в системах и приложениях.
A.13.1.2	Безопасность сетевых сервисов	*Средства реализации* Должны быть определены для всех сетевых услуг и включены в соглашения по обслуживанию сетей механизмы обеспечения безопасности, уровни сервиса и требования к управлению, осуществляются ли эти услуги внутренними подразделениями или сторонней организацией.
A.13.1.3	Разделение в сетях	*Средства реализации* 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	Политики и процедуры передачи информации	*Средства реализации* Должны быть разработаны политики, процедуры и средства управления для защиты передачи информации, осуществляемой посредством любых типов коммуникационного оборудования.
A.13.2.2	Соглашения по передаче информации	*Средства реализации* Соглашения должны регламентировать безопасную передачу бизнес-информации между организацией и внешними сторонами.
A.13.2.3	Электронные сообщения	*Средства реализации* Информация, передаваемая электронными сообщениями, должна быть соответствующим образом защищена.
A.13.2.4	Соглашения о конфиденциальности или неразглашении	*Средства реализации* 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 установление требований по информационной безопасности	*Средства реализации* 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 услуг в сетях общего пользования	*Средства реализации* Информация, используемая прикладными услугами, передающаяся по общедоступным сетям, должна быть защищена от мошеннических действий, претензий, связанных с нарушениями контрактных обязательств, и несанкционированного раскрытия и изменения.

A.14.1.3	Защита операций прикладных услуг	*Средства реализации* Информация, участвующая в операциях, осуществляемых при пользовании прикладными услугами, должна быть защищена с целью предотвращения незавершенной передачи, неправильной маршрутизации, несанкционированного изменения сообщения, несанкционированного раскрытия, несанкционированного дублирования сообщения или воспроизведения.
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 безопасности при разработке	*Средства реализации* Правила для разработки программного обеспечения и систем должны быть установлены и применяться ко всем разработкам в организации.
A.14.2.2	Процедуры управления системными изменениями	*Средства реализации* Изменения в системах в течение цикла разработки должны быть управляемыми посредством формализованных процедур управления изменениями.
A.14.2.3	Технический анализ приложений после изменений операционной платформы	*Средства реализации* После изменения операционных платформ, 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 в пакетах программ	*Средства реализации* 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 защищенных систем	*Средства реализации* Принципы разработки защищенных систем должны быть установлены, документированы, поддерживаться и применяться во всех случаях внедрения информационных систем.
A.14.2.6	Безопасная среда разработки	*Средства реализации* Организации должны обеспечивать и соответствующим образом защищать безопасные среды разработки и интеграции систем, охватывающие весь цикл разработки.

A.14.2.7	Разработка, переданная на аутсорсинг	*Средства реализации* Организация должна контролировать и вести мониторинг процесса разработки системы, переданного на аутсорсинг.
A.14.2.8	Тестирование защищенности системы	*Средства реализации* В ходе разработки должно выполняться тестирование функциональности, связанной с безопасностью.
A.14.2.9	Приемочное тестирование системы	*Средства реализации* 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 при тестировании.		
A.14.3.1	Защита данных для тестирования	*Средства реализации* 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* 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	Решение вопросов безопасности в соглашениях с поставщиками	*Средства реализации* Все существенные требования по информационной безопасности должны быть установлены и согласованы с каждым поставщиком, который может получать доступ, обрабатывать, хранить, передавать информацию организации или поставлять компоненты для ИТ-инфраструктуры.
A.15.1.3	Цепочка поставок информационно-коммуникационных технологий	*Средства реализации* Соглашения с поставщиками должны включать требования, учитывающие риски информационной безопасности, связанные с цепочкой поставок услуг и продуктов в сфере информационно-коммуникационных технологий.
A.15.2 Управление предоставлением услуги поставщиком		
Задача: поддерживать согласованный уровень информационной безопасности и предоставления услуги в соответствии с соглашениями с поставщиком.		

A.15.2.1	Мониторинг и анализ услуг поставщика	*Средства реализации* Организации должны регулярно отслеживать, анализировать и проводить аудит предоставления услуги поставщиком.
A.15.2.2	Управление изменениями в услугах поставщика	*Средства реализации* Необходимо управлять изменениями в предоставлении услуг поставщиками, включая поддержание и улучшение существующих политик информационной безопасности, процедур и средств управления, с учетом критичности бизнес-информации, используемых систем и процессов и повторной оценки рисков.
A.16 Управление инцидентами 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	Обязанности и процедуры	*Средства реализации* Должна быть установлены обязанности руководства и процедуры, чтобы гарантировать быстрый, результативный и надлежащий ответ на инциденты информационной безопасности.
A.16.1.2	Оповещение о событиях, связанных с информационной безопасностью	*Средства реализации* Оповещение о событиях информационной безопасности должно доводиться по соответствующим каналам управления как можно быстрее.
A.16.1.3	Оповещение об уязвимостях в информационной безопасности	*Средства реализации* От сотрудников и работающих по контракту, использующих информационные системы и сервисы организации, необходимо требовать фиксировать и докладывать о любых обнаруженных или предполагаемых уязвимостях в информационной безопасности систем и сервисов.
A.16.1.4	Оценка и решение по событиям информационной безопасности	*Средства реализации* События информационной безопасности должны оцениваться и затем приниматься решение, следует ли их классифицировать как инцидент информационной безопасности.
A.16.1.5	Ответные меры на инциденты информационной безопасности	*Средства реализации* Реагирование на инциденты информационной безопасности должно осуществляться в соответствии с документированными процедурами.

A.16.1.6	Излечение уроков из инцидентов информационной безопасности	*Средства реализации* 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* Организация должна определить и применять процедуры для идентификации, сбора, комплектования и сохранения информации, которая может служить в качестве свидетельств.
A.17 Аспекты информационной безопасности в менеджменте непрерывности бизнеса		
A.17.1 Непрерывность информационной безопасности		
Задача: Непрерывность информационной безопасности должна быть встроена в систему менеджмента непрерывностью бизнеса организации.		
A.17.1.1	Планирование непрерывности информационной безопасности	*Средства реализации* Организация должна определить свои требования к информационной безопасности и управлению непрерывностью информационной безопасности в неблагоприятных ситуациях, например, во время кризиса или чрезвычайной ситуации.
A.17.1.2	Обеспечение непрерывности информационной безопасности	*Средства реализации* 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* Организация должна проверять разработанные и внедренные средства управления непрерывностью информационной безопасности через определенные интервалы времени, чтобы гарантировать, что эти средства пригодны и результативны во время неблагоприятных ситуаций.
A.17.2 Резервирование		
Задача: гарантировать возможность применения средств обработки информации.		
A.17.2.1	Возможность применения средств обработки информации	*Средства реализации* Средства обработки информации должны устанавливаться с избыточностью, достаточной для обеспечения требований по возможности применения.
A.18 Соответствие		
A.18.1 Соответствие законодательным и контрактным требованиям		

Задача: избегать нарушений законодательных, нормативных или контрактных обязательств, имеющих отношение к информационной безопасности, и любых требований безопасности.		
A.18.1.1	Определение действующих законодательных и контрактных требований	*Средства реализации* Все соответствующие законодательные, нормативные, контрактные требования, а также подход организации к удовлетворению этих требований должны быть явным образом определены, документированы и сохраняться актуальными для каждой информационной системы и организации.
A.18.1.2	Права интеллектуальной собственности	*Средства реализации* Должны выполняться соответствующие процедуры, чтобы гарантировать соответствие законодательным, нормативным и контрактным требованиям, связанным с правами на интеллектуальную собственность и использованием программных продуктов, защищенных авторским правом.
A.18.1.3	Защита записей	*Средства реализации* Записи должны быть защищены от потери, повреждения, фальсификации, несанкционированного доступа и несанкционированной публикации в соответствии с законодательными, нормативными, контрактными требованиями и требованиями бизнеса.
A.18.1.4	Конфиденциальность и защита персональных данных	*Средства реализации* Конфиденциальность и защита персональных данных должны быть обеспечены в той мере, в какой это требуется соответствующим законодательством и нормативными актами, где это применимо.
A.18.1.5	Регламентация применения криптографических методов	*Средства реализации* Криптографические методы должны использоваться в соответствии со всеми действующими соглашениями, законодательными и нормативными актами.
A.18.2 Анализ информационной безопасности		
Задача: гарантировать, что средства обеспечения информационной безопасности внедрены и используются в соответствии с организационной политикой и процедурами.		

A.18.2.1	Независимый анализ информационной безопасности	*Средства реализации* Подход организации к управлению информационной безопасностью и его реализация (т. е. задачи управления, средства управления, политики, процессы и процедуры по обеспечению информационной безопасности) должны подвергаться независимому анализу через запланированные интервалы времени или в тех случаях, когда происходят существенные изменения.
A.18.2.2	Соответствие политикам безопасности и стандартам	*Средства реализации* Руководители в пределах своей области ответственности должны регулярно анализировать соответствие обработки информации и процедур политикам безопасности, стандартам и любым другим требованиям по безопасности.
A.18.2.3	Анализ технического соответствия	*Средства реализации* Информационные системы должны регулярно анализироваться на соответствие политикам и стандартам информационной безопасности организации.

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