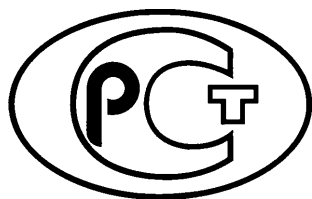


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ



НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

**ГОСТР
ИСО/МЭК 27001—
2021**

Информационная технология
МЕТОДЫ И СРЕДСТВА
ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

**Системы менеджмента
информационной безопасности.
Требования**

(ISO/IEC 27001:2013, ЮТ)

Издание официальное

Москва
Российский институт стандартизации
2021

Предисловие

1 ПОДГОТОВЛЕН Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Открытым акционерным обществом «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТекС») и Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России») на основе официального перевода на русский язык англоязычной версии указанного в пункте 4 стандарта, который выполнен ФГБУ «РСТ»

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2021 г. № 1653-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27001:2013 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (ISO/IEC 27001:2013 «Information technology — Security techniques — Information security management systems — Requirements», IDT), включая технические поправки: Cor. 1:2014; Cor. 2:2015.

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

Дополнительные сноски в тексте стандарта, выделенные курсивом, приведены для пояснения текста оригинала

5 ВЗАМЕН ГОСТ Р ИСО/МЭК 27001—2006

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

© ISO, 2013

© IEC, 2013

© Оформление. ФГБУ «РСТ», 2021

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

Содержание

1	Область применения.....	1
2	Нормативные ссылки.....	1
3	Термины и определения.....	1
4	Контекст деятельности организации.....	1
4.1	Понимание внутренних и внешних факторов деятельности организации.....	1
4.2	Понимание потребностей и ожиданий заинтересованных сторон.....	2
4.3	Определение области действия системы менеджмента информационной безопасности.....	2
4.4	Система менеджмента информационной безопасности.....	2
5	Руководство.....	2
5.1	Лидерство и приверженность.....	2
5.2	Политика.....	2
5.3	Роли, обязанности и полномочия в организации.....	3
6	Планирование.....	3
6.1	Действия по рассмотрению рисков и возможностей.....	3
6.2	Цели информационной безопасности и планы по их достижению.....	4
7	Обеспечение и поддержка.....	5
7.1	Ресурсы.....	5
7.2	Квалификация.....	5
7.3	Осведомленность.....	5
7.4	Взаимодействие.....	5
7.5	Документированная информация.....	6
8	Функционирование.....	6
8.1	Оперативное планирование и контроль.....	6
8.2	Оценка рисков информационной безопасности.....	7
8.3	Обработка рисков информационной безопасности.....	7
9	Оценивание исполнения.....	7
9.1	Мониторинг, оценка защищенности, анализ и оценивание.....	7
9.2	Внутренний аудит.....	7
9.3	Проверка со стороны руководства.....	8
10	Улучшение.....	8
10.1	Несоответствие и корректирующие действия.....	8
10.2	Постоянное улучшение.....	8
	Приложение А (обязательное) Меры обеспечения информационной безопасности и цели их применения.....	9
	Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам.....	21
	Библиография.....	22

Введение

Настоящий стандарт подготовлен с целью установления требований по созданию, внедрению, поддержке и постоянному улучшению системы менеджмента информационной безопасности. Решение о внедрении системы менеджмента информационной безопасности является стратегическим решением организации. На то, в каком виде в организации будет создана и внедрена система менеджмента информационной безопасности, влияют потребности и цели деятельности организации, требования безопасности, реализуемые организацией процессы деятельности, а также размеры и структура организации. Предполагается, что все указанные факторы влияния изменяются со временем.

Система менеджмента информационной безопасности сохраняет конфиденциальность, целостность и доступность информации за счет применения процесса управления рисками и дает заинтересованным сторонам¹⁾ уверенность в том, что риски надлежащим образом управляются.

Важно, чтобы система менеджмента информационной безопасности организации составляла часть процессов и структуры управления организации и была интегрирована с ними. Также важно, чтобы информационная безопасность учитывалась при проектировании процессов, информационных систем и средств управления. Предполагается, что система менеджмента информационной безопасности будет адаптироваться к потребностям организации.

Настоящий стандарт может быть использован заинтересованными сторонами для оценки способности организации соответствовать собственным требованиям к информационной безопасности.

Порядок представления требований в настоящем стандарте не отражает их значимость и последовательность, в соответствии с которыми они должны быть реализованы. Нумерация требований приведена только для ссылочных целей.

Обзор и терминология систем менеджмента информационной безопасности со ссылками на семейство стандартов системы менеджмента информационной безопасности (включая ИСО/МЭК 27003 [2], ИСО/МЭК 27004 [3] и ИСО/МЭК 27005 [4]), содержащих соответствующие термины и определения, представлены в ИСО/МЭК 27000.

Настоящий стандарт использует высокоуровневую структуру, идентичные названия подразделов, идентичный текст, общие термины и основные определения, приведенные в приложении SL документа «Директивы ИСО/МЭК, часть 1» [6], и соответственно поддерживает совместимость с другими стандартами по системам менеджмента, соответствующим приложению SL.

Общий подход, определенный в приложении SL, будет полезен для тех организаций, которые решили использовать единую систему менеджмента, отвечающую требованиям двух и более стандартов по системам менеджмента.

¹⁾ *Заинтересованная сторона (interested party) — лицо или организация, которые могут воздействовать на осуществление деятельности или принятие решения, быть подверженными их воздействию или воспринимать себя в качестве последних (см. ГОСТ Р ИСО 9000—2015, пункт 3.2.3).*

ГОСТ Р ИСО/МЭК 27001—2021**НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ****Информационная технология****МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ****Системы менеджмента информационной безопасности.
Требования**

Information technology. Security techniques. Information security management systems. Requirements

Дата введения — 2022—01—01**1 Область применения**

Настоящий стандарт устанавливает общие требования по созданию, внедрению, поддержке и постоянному улучшению системы менеджмента информационной безопасности в контексте деятельности организации. Настоящий стандарт также содержит требования по оценке и обработке рисков информационной безопасности с учетом потребностей организации. Изложенные в настоящем стандарте требования являются обобщенными и предназначены для применения во всех организациях независимо от их типа, размера, структуры и сферы деятельности. Исключение любого из требований, указанных в разделах 4—10, не допускается, если организация заявляет о соответствии данному стандарту.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты [для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных — последнее издание (включая все изменения)]:

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

3 Термины и определения

В настоящем стандарте применяются термины и определения, приведенные в ИСО/МЭК 27000.

4 Контекст деятельности организации**4.1 Понимание внутренних и внешних факторов деятельности организации**

В организации должны быть определены внешние и внутренние факторы, имеющие отношение к деятельности организации и оказывающие влияние на ее способность достигать ожидаемого(ых) результата(ов) от системы менеджмента информационной безопасности.

Примечание — Определение этих факторов относится к установлению внутреннего и внешнего контекста организации, рассматриваемого в ИСО 31000:2009 [5] (подраздел 5.3).

ГОСТ Р ИСО/МЭК 27001—2021**4.2 Понимание потребностей и ожиданий заинтересованных сторон**

Организация должна определить:

- а) заинтересованные стороны, имеющие отношение к системе менеджмента информационной безопасности;
- б) требования этих заинтересованных сторон к информационной безопасности.

Примечание — Требования заинтересованных сторон могут включать правовые и нормативные требования и договорные обязательства.

4.3 Определение области действия системы менеджмента информационной безопасности

Для установления области действия системы менеджмента информационной безопасности организация должна определить применимость системы менеджмента информационной безопасности и ее границы.

При определении области действия системы менеджмента информационной безопасности необходимо учитывать:

- а) внутренние и внешние факторы, указанные в 4.1;
- б) требования, приведенные в 4.2;
- в) порядок взаимодействия и зависимости между деятельностью данной организации и деятельностью других организаций.

Область действия системы менеджмента информационной безопасности должна быть доступна в виде документированной информации.

4.4 Система менеджмента информационной безопасности

Создание, внедрение, поддержку и постоянное улучшение системы менеджмента информационной безопасности организация должна проводить в соответствии с требованиями настоящего стандарта.

5 Руководство**5.1 Лидерство и приверженность**

Высшее руководство организации должно демонстрировать свое лидерство и приверженность в отношении системы менеджмента информационной безопасности:

- а) установлением политики и целей информационной безопасности, совместимых со стратегическим направлением развития организации;
- б) интеграцией требований системы менеджмента информационной безопасности в процессы организации;
- в) доступностью ресурсов, необходимых для системы менеджмента информационной безопасности;
- г) декларированием важности обеспечения эффективного менеджмента информационной безопасности и соответствия требованиям системы менеджмента информационной безопасности;
- д) достижением системой менеджмента информационной безопасности ожидаемых результатов;
- е) направляя и поддерживая лиц, способствующих повышению результативности системы менеджмента информационной безопасности;
- ж) постоянным улучшением системы менеджмента информационной безопасности;
- з) поддержкой других руководителей в реализации их ведущих ролей в рамках зон их ответственности.

5.2 Политика

Высшее руководство организации должно установить политику информационной безопасности, которая:

- а) соответствует целям деятельности организации;
- б) содержит цели информационной безопасности (см. 6.2) или обеспечивает основу для их установления;
- в) содержит обязательство соответствовать применимым требованиям, относящимся к информационной безопасности;

ГОСТ Р ИСО/МЭК 27001—2021

д) содержит обязательство постоянно улучшать систему менеджмента информационной безопасности.

Политика информационной безопасности должна быть:

- е) доступна в виде документированной информации;
- ф) доведена до сведения работников организации;
- д) доступна заинтересованным сторонам.

5.3 Роли, обязанности и полномочия в организации

Высшее руководство организации должно обеспечить назначение обязанностей и полномочий для ролей, имеющих отношение к обеспечению информационной безопасности, и доведение этих обязанностей и полномочий до всех заинтересованных сторон.

Высшее руководство должно назначать обязанности и полномочия:

- а) для обеспечения уверенности в соответствии системы менеджмента информационной безопасности организации требованиям настоящего стандарта;
- б) представления отчетности о функционировании системы менеджмента информационной безопасности высшему руководству.

Примечание — Высшее руководство также может устанавливать обязанности и полномочия для представления отчетности о функционировании системы менеджмента информационной безопасности в рамках организации.

6 Планирование**6.1 Действия по рассмотрению рисков и возможностей****6.1.1 Общие положения**

При планировании системы менеджмента информационной безопасности организация должна учитывать факторы, указанные в 4.1, и требования, приведенные в 4.2, а также определять подлежащие рассмотрению риски информационной безопасности и возможности организации для:

- а) обеспечения уверенности в том, что система менеджмента информационной безопасности способна достичь намеченных результатов;

- б) предотвращения или уменьшения нежелательных последствий¹⁾;
- с) обеспечения постоянного улучшения²⁾.

Организация должна планировать:

- д) действия по рассмотрению данных рисков и возможностей;
- е) каким образом:

- 1) интегрировать и внедрять эти действия в процессы системы менеджмента информационной безопасности;
- 2) оценивать результативность этих действий.

6.1.2 Оценка рисков информационной безопасности

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

- а) устанавливать и поддерживать критерии рисков информационной безопасности, включая:
 - 1) критерии принятия рисков информационной безопасности;
 - 2) критерии для проведения оценки рисков информационной безопасности;
- б) обеспечивать уверенность в том, что повторные оценки рисков информационной безопасности дают непротиворечивые, достоверные и сопоставимые результаты;
- с) идентифицировать риски информационной безопасности, т. е.:
 - 1) применять процесс оценки рисков информационной безопасности для идентификации рисков, связанных с нарушением конфиденциальности, целостности и доступности информации в рамках области действия системы менеджмента информационной безопасности;
 - 2) идентифицировать владельцев рисков информационной безопасности;

¹⁾ Например, реализации рисков информационной безопасности.

²⁾ Например, уровня информационной безопасности.

ГОСТ Р ИСО/МЭК 27001—2021

- d) проводить анализ рисков информационной безопасности, т. е.:
- 1) оценивать потенциальные последствия, которые могут произойти в результате реализации рисков информационной безопасности, идентифицированных в соответствии с 6.1.2 с) 1);
 - 2) оценивать реальную вероятность реализации рисков информационной безопасности, идентифицированных в соответствии с 6.1.2 с) 1);
 - 3) определять уровни рисков информационной безопасности;
- e) оценивать риски информационной безопасности, т. е.:
- 1) сравнивать результаты анализа рисков информационной безопасности с критериями рисков, установленными в соответствии с 6.1.2 а);
 - 2) определять приоритетность обработки проанализированных рисков информационной безопасности.

Организация должна хранить документированную информацию о процессе оценки рисков информационной безопасности.

6.1.3 Обработка рисков информационной безопасности

Организация должна определить и применять процесс обработки рисков информационной безопасности:

- a) для выбора подходящих вариантов обработки рисков информационной безопасности, учитывая результаты оценки рисков информационной безопасности;
- б) определения всех мер и средств информационной безопасности, необходимых для реализации выбранного(ых) варианта(ов) обработки рисков информационной безопасности.

Примечание — При необходимости организация может разрабатывать меры обеспечения информационной безопасности или взять их из любого источника;

- с) сравнения мер и средств информационной безопасности, определенных в соответствии с 6.1.3 б), с указанными в приложении А для проверки того, что никакие необходимые меры обеспечения информационной безопасности не были упущены.

Примечание 1 — Приложение А содержит базовый перечень мер и средств информационной безопасности и целей их применения. Пользователям настоящего стандарта следует обращаться к приложению А для обеспечения уверенности в том, что никакие необходимые меры обеспечения информационной безопасности не были упущены.

Примечание 2 — Цели применения мер и средств информационной безопасности неявным образом включены в выбранные меры обеспечения информационной безопасности. Приведенные в приложении А меры обеспечения информационной безопасности и цели их применения не являются исчерпывающими, и организация может рассматривать необходимость дополнительных мер и средств информационной безопасности и целей их применения;

- d) подготовки ведомости применимости мер и средств информационной безопасности, которая содержит¹⁾:
 - необходимые меры обеспечения информационной безопасности [см. 6.1.3 б) и с)];
 - обоснования их применения;
 - информацию о том, реализованы или нет необходимые меры обеспечения информационной безопасности;
 - обоснования неприменения мер и средств информационной безопасности, представленных в приложении А;
- e) разработки плана обработки рисков информационной безопасности;
- ф) согласования и (или) утверждения плана обработки рисков информационной безопасности и принятия остаточных рисков информационной безопасности владельцами рисков.

Организация должна хранить документированную информацию о процессе обработки рисков информационной безопасности.

Примечание — Процесс оценки и обработки рисков информационной безопасности в настоящем стандарте согласуется с принципами и общими рекомендациями, представленными в ИСО 31000 [5].

6.2 Цели информационной безопасности и планы по их достижению

В организации должны быть установлены цели обеспечения информационной безопасности применительно к соответствующим функциям и уровням управления организацией.

¹⁾ Пункт 6.1.3 d) приведен с учетом технической правки к ISO/IEC 27001:2013.

ГОСТ Р ИСО/МЭК 27001—2021

Цели информационной безопасности должны:

- а) быть согласованы с политикой информационной безопасности;
- б) быть измеримыми (если это практически возможно);
- в) учитывать применимые требования информационной безопасности и результаты оценки и обработки рисков информационной безопасности;
- г) быть доведены до сведения всех заинтересованных сторон;
- е) обновляться по мере необходимости.

Организация должна хранить документированную информацию о целях информационной безопасности.

При планировании способов достижения своих целей информационной безопасности организация должна определить:

- ф) что должно быть сделано;
- д) какие ресурсы потребуются;
- г) кто будет нести ответственность;
- и) когда планируемое мероприятие будет завершено;
- ж) как будут оцениваться результаты.

7 Обеспечение и поддержка

7.1 Ресурсы

Организация должна определить и обеспечить наличие ресурсов, необходимых для создания, внедрения, поддержки и постоянного улучшения системы менеджмента информационной безопасности.

7.2 Квалификация

Организация должна:

- а) определить необходимую квалификацию для лиц(а), выполняющих(его) работу под ее контролем, которая влияет на обеспечение ее информационной безопасности;
- б) убедиться, что квалификация этих лиц базируется на их приемлемом образовании, профессиональной подготовке (стажировке) или опыте работы;
- в) при необходимости принимать меры по получению необходимой квалификации и проводить оценивание результативности принятых мер;
- г) сохранять соответствующую документированную информацию в качестве свидетельств наличия необходимой квалификации.

Примечание — Применяемые меры могут включать, например, проведение тренинга, наставничество или перераспределение обязанностей среди имеющихся работников, а также наем или привлечение к работам по контракту лиц, имеющих необходимую квалификацию.

7.3 Осведомленность

Лица, выполняющие работу под контролем организации, должны быть осведомлены:

- а) о политике информационной безопасности организации;
- б) их вкладе в обеспечение результативности системы менеджмента информационной безопасности, включая пользу от улучшения деятельности по обеспечению информационной безопасности;
- в) последствиях несоблюдения требований системы менеджмента информационной безопасности.

7.4 Взаимодействие

В организации должна быть определена необходимость во взаимодействии внутри организации и с внешними сторонами по вопросам, имеющим отношение к системе менеджмента информационной безопасности, включая следующие:

- а) предмет взаимодействия;
- б) когда взаимодействовать;
- в) с кем взаимодействовать;
- г) кто должен взаимодействовать;
- е) процедуры осуществления взаимодействия.

ГОСТ Р ИСО/МЭК 27001—2021**7.5 Документированная информация****7.5.1 Общие положения**

Система менеджмента информационной безопасности организации должна включать:

- а) документированную информацию, требуемую в соответствии с настоящим стандартом;
- б) документированную информацию, определяемую организацией как необходимую для обеспечения результативности системы менеджмента информационной безопасности.

Примечание — Объем документированной информации, относящейся к системе менеджмента информационной безопасности, в разных организациях может быть различным, в зависимости:

- а) от размеров организации и вида ее деятельности, процессов, продуктов и услуг;
- б) сложности процессов и их взаимодействия;
- с) квалификации персонала.

7.5.2 Создание и обновление документированной информации

При создании и обновлении документированной информации организация должна обеспечить надлежащие:

- а) идентификацию и описание (например, наименование, дата, автор или номер для ссылок);
- б) формат (например, язык, версия программного обеспечения, графика) и носитель информации (например, бумажный, электронный);
- с) проверку и подтверждение ее пригодности и адекватности.

7.5.3 Управление документированной информацией

Требуется осуществлять управление документированной информацией, необходимой для системы менеджмента информационной безопасности и указанной в настоящем стандарте, с целью обеспечения ее:

- а) доступности и пригодности для использования, когда и где это необходимо;
- б) надлежащей защиты (например, от нарушения конфиденциальности, ненадлежащего использования или нарушения целостности).

Для управления документированной информацией организация должна осуществлять следующие (если это применимо) действия по отношению к ней:

- с) распространение, обеспечение доступа, поиска и использования;
- д) хранение и обеспечение сохранности, включая сохранение разборчивости;
- е) управление изменениями (например, управление версиями);
- ф) архивное хранение и уничтожение.

Организация должна идентифицировать и управлять необходимой для осуществления планирования и функционирования системы менеджмента информационной безопасности документированной информацией из внешних источников.

Примечание — Доступ к документированной информации предполагает либо наличие полномочий только на ее просмотр, либо на просмотр и внесение изменений в документированную информацию, а также другие действия.

8 Функционирование**8.1 Оперативное планирование и контроль**

Организация должна планировать, реализовывать и контролировать процессы, необходимые для соответствия требованиям информационной безопасности и для осуществления действий, определенных в 6.1. Организация должна также реализовывать планы по достижению целей информационной безопасности, определенных в соответствии с 6.2.

Организация должна хранить документированную информацию в объеме, необходимом для обеспечения уверенности в том, что процессы были выполнены в соответствии с планами.

В организации необходимо управлять запланированными изменениями системы менеджмента информационной безопасности и анализировать последствия незапланированных изменений, принимая при необходимости меры по снижению любых неблагоприятных последствий.

ГОСТ Р ИСО/МЭК 27001—2021

Процессы организации, осуществляемые с использованием аутсорсинга¹⁾, должны быть определены и проконтролированы.

8.2 Оценка рисков информационной безопасности

Организация должна проводить оценку рисков информационной безопасности через запланированные интервалы времени или в случае предполагаемых или произошедших существенных изменений, учитывая критерии рисков информационной безопасности, установленные в соответствии с 6.1.2 а).

Организация должна хранить документированную информацию о результатах проведенных оценок рисков информационной безопасности.

8.3 Обработка рисков информационной безопасности

Организация должна реализовать план обработки рисков информационной безопасности.

Организация должна хранить документированную информацию о результатах обработки рисков информационной безопасности.

9 Оценивание исполнения**9.1 Мониторинг, оценка защищенности, анализ и оценивание**

Организация должна оценивать деятельность по обеспечению информационной безопасности, а также результативность системы менеджмента информационной безопасности.

Организация должна определить:

а) объекты мониторинга и оценки защищенности, включая процессы, меры обеспечения информационной безопасности;

б) методы проведения мониторинга, оценки защищенности, анализа и оценивания, обеспечивающие уверенность в достоверности результатов.

Примечание — Допустимыми признаются методы, дающие сопоставимые и воспроизводимые результаты;

с) когда проводить мониторинг и оценку защищенности;

д) кто должен осуществлять мониторинг и оценку защищенности;

е) когда анализировать результаты мониторинга и оценки защищенности;

ф) кто должен осуществлять анализ и оценивание этих результатов.

Организация должна хранить соответствующую документированную информацию в качестве свидетельства результатов мониторинга и оценки защищенности.

9.2 Внутренний аудит

Организация должна через запланированные интервалы времени проводить внутренние аудиты с целью определения, насколько система менеджмента информационной безопасности:

а) соответствует:

1) собственным требованиям организации к системе менеджмента информационной безопасности;

2) требованиям настоящего стандарта;

б) эффективно реализована и поддерживается.

Организация должна:

с) планировать, разрабатывать, реализовывать и поддерживать программу(ы) аудита, включая определение периодичности и методов проведения аудита, ответственность, требования к планированию и предоставление отчетности аудита. Программа(ы) аудита должна(ы) учитывать значимость проверяемых процессов и результаты предыдущих аудитов;

д) определять критерии и область проведения каждого аудита;

е) выбирать аудиторов и сопровождать проведение аудитов для обеспечения уверенности в объективности и беспристрастности процесса аудита;

¹⁾ Аутсорсинг — передача одним юридическим лицом (контрактором) другому юридическому лицу (субконтрактору) работ или услуг и принятие их к выполнению этим другим юридическим лицом (субконтрактором) на основании договора (см. Решение Совета Евразийской экономической комиссии от 21 декабря 2016 г. № 143 «О Концепции создания евразийской сети промышленной кооперации и субконтрактации»).

ГОСТ Р ИСО/МЭК 27001—2021

- ф) обеспечивать предоставление результатов аудитов соответствующим руководителям организации;
- д) хранить документированную информацию в качестве свидетельств реализации программ(ы) аудита и результатов аудита.

9.3 Проверка со стороны руководства

Высшее руководство должно проводить проверку системы менеджмента информационной безопасности через запланированные интервалы времени в целях обеспечения уверенности в сохраняющейся ее приемлемости, адекватности и результативности.

Проверка со стороны руководства должна включать рассмотрение:

- а) состояния выполнения решений по результатам предыдущих проверок со стороны руководства;
- б) изменений внешних и внутренних факторов, касающихся системы менеджмента информационной безопасности;
- с) отзывов о результатах деятельности по обеспечению информационной безопасности, включая тенденции:
 - 1) в выявлении несоответствий и применении корректирующих действий;
 - 2) результатах мониторинга и оценки защищенности;
 - 3) результатах аудита;
 - 4) достижении целей информационной безопасности;
- д) отзывов от заинтересованных сторон;
- е) результатов оценки рисков информационной безопасности и статуса выполнения плана обработки рисков информационной безопасности;
- ф) возможностей для постоянного улучшения системы менеджмента информационной безопасности.

Результаты проверки со стороны руководства должны включать решения, относящиеся к возможностям постоянного улучшения и к необходимости внесения любых изменений в систему менеджмента информационной безопасности организации.

Организация должна хранить документированную информацию в качестве свидетельства результатов проверок со стороны руководства.

10 Улучшение**10.1 Несоответствие и корректирующие действия**

При появлении несоответствия организация должна:

- а) реагировать на несоответствие и, если применимо:
 - 1) предпринять необходимые действия, чтобы контролировать и устранить его;
 - 2) устранять последствия несоответствия;
- б) оценивать необходимость корректирующих действий по устранению причин несоответствия, чтобы избежать его повторения или появления в другом месте посредством:
 - 1) анализа несоответствия;
 - 2) определения причин появления несоответствия;
 - 3) определения наличия подобных несоответствий или потенциальных(ой) возможностей(и) их возникновения;
- с) выполнять необходимые корректирующие действия;
- д) анализировать результативность предпринятых корректирующих действий;
- е) вносить при необходимости изменения в систему менеджмента информационной безопасности.

Корректирующие действия должны быть адекватны последствиям выявленных несоответствий.

Организация должна хранить документированную информацию в качестве свидетельства:

- ф) о характере несоответствий и любых последующих предпринимаемых действиях;
- д) результатах любых корректирующих действий.

10.2 Постоянное улучшение

Организация должна постоянно улучшать приемлемость, адекватность и результативность системы менеджмента информационной безопасности.

**Приложение А
(обязательное)**

Меры обеспечения информационной безопасности и цели их применения

Перечисленные в таблице А.1 цели, а также меры обеспечения информационной безопасности непосредственно заимствованы и полностью соответствуют целям, мерам и средствам информационной безопасности, приведенным в ИСО/МЭК 27002:2013 [1] (разделы 5—18), и должны быть использованы, как определено в 6.1.3.

Таблица А.1 — Меры обеспечения информационной безопасности и цели их применения

А.5 Политики информационной безопасности		
А.5.1 Руководящие указания в части информационной безопасности		
Цель: обеспечить управление и поддержку высшим руководством информационной безопасности в соответствии с требованиями бизнеса, соответствующих законов и нормативных актов		
А.5.1.1	Политики информационной безопасности	<i>Мера обеспечения информационной безопасности</i> Совокупность политик информационной безопасности должна быть определена, утверждена руководством, опубликована и доведена до сведения всех работников организации и соответствующих внешних сторон
А.5.1.2	Пересмотр политик информационной безопасности	<i>Мера обеспечения информационной безопасности</i> Политики информационной безопасности должны пересматриваться через запланированные интервалы времени или в случае происходящих существенных изменений для обеспечения уверенности в сохранении их приемлемости, адекватности и результативности
А.6 Организация деятельности по информационной безопасности		
А.6.1 Внутренняя организация деятельности по обеспечению информационной безопасности		
Цель: создать структуру органов управления для инициирования и контроля внедрения и функционирования информационной безопасности в организации		
А.6.1.1	Роли и обязанности по обеспечению информационной безопасности	<i>Мера обеспечения информационной безопасности</i> Все обязанности по обеспечению информационной безопасности должны быть определены и распределены
А.6.1.2	Разделение обязанностей	<i>Мера обеспечения информационной безопасности</i> Пересекающиеся обязанности и зоны ответственности должны быть разделены для уменьшения возможности несанкционированного или непреднамеренного изменения или нецелевого использования активов организации
А.6.1.3	Контакт с органами власти	<i>Мера обеспечения информационной безопасности</i> Следует поддерживать соответствующие контакты с уполномоченными органами
А.6.1.4	Взаимодействие с заинтересованными профессиональными группами	<i>Мера обеспечения информационной безопасности</i> Следует поддерживать соответствующее взаимодействие с заинтересованными профессиональными группами и ассоциациями или форумами, проводимыми специалистами по безопасности
А.6.1.5	Информационная безопасность при управлении проектом	<i>Мера обеспечения информационной безопасности</i> Информационную безопасность следует рассматривать при управлении проектом независимо от типа проекта
А.6.2 Мобильные устройства и дистанционная работа		
Цель: обеспечить безопасность при дистанционной работе и использовании мобильных устройств		
А.6.2.1	Политика использования мобильных устройств	<i>Мера обеспечения информационной безопасности</i> Следует определить политику и реализовать поддерживающие меры безопасности для управления рисками информационной безопасности, связанными с использованием мобильных устройств

ГОСТ Р ИСО/МЭК 27001—2021

Продолжение таблицы А. 1

А.6.2.2	Дистанционная работа	<i>Мера обеспечения информационной безопасности</i> Следует определить политику и реализовать поддерживающие меры безопасности для защиты информации, доступ к которой, обработка или хранение осуществляются в местах дистанционной работы
А.7 Безопасность, связанная с персоналом		
А.7.1 При приеме на работу Цель: обеспечить уверенность в том, что работники и подрядчики понимают свои обязанности и подходят для роли, на которую они рассматриваются		
А.7.1.1	Проверка	<i>Мера обеспечения информационной безопасности</i> Проверку всех кандидатов при приеме на работу следует осуществлять согласно соответствующим законам, правилам и этическим нормам. Проверка должна быть соразмерна требованиям бизнеса, категории информации, которая будет доступна, и предполагаемым рискам информационной безопасности
А.7.1.2	Правила и условия работы	<i>Мера обеспечения информационной безопасности</i> В договорных соглашениях с работниками и подрядчиками должны быть установлены их обязанности и обязанности организации по обеспечению информационной безопасности
А.7.2 Во время работы Цель: обеспечить уверенность в том, что работники и подрядчики осведомлены о своих обязанностях в отношении информационной безопасности и выполняют их		
А.7.2.1	Обязанности руководства организации	<i>Мера обеспечения информационной безопасности</i> Руководство организации должно требовать от всех работников и подрядчиков соблюдения информационной безопасности в соответствии с установленными в организации политиками и процедурами
А.7.2.2	Осведомленность, обучение и практическая подготовка (тренинги) в области информационной безопасности	<i>Мера обеспечения информационной безопасности</i> Все работники организации и при необходимости подрядчики должны быть надлежащим образом обучены, практически подготовлены и на регулярной основе осведомлены об обновлениях политик и процедур информационной безопасности организации, необходимых для выполнения их функциональных обязанностей
А.7.2.3	Дисциплинарный процесс	<i>Мера обеспечения информационной безопасности</i> Должен существовать формализованный и доведенный до персонала дисциплинарный процесс по принятию мер в отношении работников, совершивших нарушение информационной безопасности
А.7.3 Увольнение и смена места работы Цель: защита интересов организации при смене места работы или увольнении работника		
А.7.3.1	Прекращение или изменение трудовых обязанностей	<i>Мера обеспечения информационной безопасности</i> Ответственность и обязанности, относящиеся к информационной безопасности, которые сохраняются после увольнения или смены места работы, должны быть определены, доведены до сведения работника или подрядчика и оформлены юридически
А.8 Менеджмент активов		
А.8.1 Ответственность за активы Цель: идентификация активов организации и определение соответствующих обязанностей по их защите		
А.8.1.1	Инвентаризация активов	<i>Мера обеспечения информационной безопасности</i> Информация, средства обработки информации и другие активы, связанные с информацией, должны быть идентифицированы, а также должен быть составлен и поддерживаться в актуальном состоянии перечень этих активов ¹⁾

¹⁾ Пункт А.8.1.1 приведен с учетом технической правки 1 к ISO/IEC 27001:2013.

ГОСТ Р ИСО/МЭК 27001—2021

Продолжение таблицы А. 1

A.8.1.2	Владение активами	<i>Мера обеспечения информационной безопасности</i> Для каждого актива, включенного в перечень инвентаризации, должен быть определен его владелец
A.8.1.3	Допустимое использование активов	<i>Мера обеспечения информационной безопасности</i> Должны быть идентифицированы, документально оформлены и реализованы правила допустимого использования активов, включая информацию и средства ее обработки
A.8.1.4	Возврат активов	<i>Мера обеспечения информационной безопасности</i> Все работники и внешние пользователи должны вернуть все активы организации, находящиеся в их пользовании, после увольнения, истечения срока действия договора или соглашения
A.8.2 Категорирование информации Цель: обеспечить уверенность в том, что в отношении информации обеспечивается надлежащий уровень защиты в соответствии с ее значимостью для организации		
A.8.2.1	Категорирование информации	<i>Мера обеспечения информационной безопасности</i> Информация должна быть категорирована с точки зрения нормативных правовых требований, ценности, критичности и чувствительности к неавторизованному раскрытию или модификации
A.8.2.2	Маркировка информации	<i>Мера обеспечения информационной безопасности</i> Должен быть разработан и реализован соответствующий набор процедур маркировки информации в соответствии с принятой в организации системой категорирования информации
A.8.2.3	Обращение с активами	<i>Мера обеспечения информационной безопасности</i> Должны быть разработаны и реализованы процедуры обращения с активами в соответствии с принятой в организации системой категорирования информации
A.8.3 Обращение с носителями информации Цель: предотвратить несанкционированное раскрытие, модификацию, удаление или уничтожение информации, хранящейся на носителях информации		
A.8.3.1	Управление сменными носителями информации	<i>Мера обеспечения информационной безопасности</i> Должны быть реализованы процедуры по управлению сменными носителями информации в соответствии с принятой в организации системой категорирования информации
A.8.3.2	Утилизация носителей информации	<i>Мера обеспечения информационной безопасности</i> При выводе из эксплуатации носителей информации требуется их надежно и безопасно утилизировать, используя формализованные процедуры
A.8.3.3	Перемещение физических носителей	<i>Мера обеспечения информационной безопасности</i> Во время транспортирования носители информации, содержащие информацию, должны быть защищены от несанкционированного доступа, неадекватного использования или повреждения
A.9 Управление доступом		
A.9.1 Требования бизнеса по управлению доступом Цель: ограничить доступ к информации и средствам ее обработки		
A.9.1.1	Политика управления доступом	<i>Мера обеспечения информационной безопасности</i> Политика управления доступом должна быть разработана, документирована и должна пересматриваться с учетом требований бизнеса и информационной безопасности
A.9.1.2	Доступ к сетям и сетевым сервисам	<i>Мера обеспечения информационной безопасности</i> Пользователям следует предоставлять доступ только к тем сетям и сетевым сервисам, на использование которых они получили конкретное разрешение

ГОСТ Р ИСО/МЭК 27001—2021

Продолжение таблицы А. 1

А.9.2 Процесс управления доступом пользователей Цель: обеспечить предоставление доступа уполномоченным пользователям и предотвратить несанкционированный доступ к системам и сервисам		
А.9.2.1	Регистрация и отмена регистрации пользователей	Мера обеспечения информационной безопасности Для назначения прав доступа должна быть реализована формализованная процедура регистрации и отмены регистрации пользователей
А.9.2.2	Предоставление пользователю права доступа	Мера обеспечения информационной безопасности Должен быть реализован формализованный процесс назначения или отмены прав доступа пользователей к системам и сервисам
А.9.2.3	Управление привилегированными правами доступа	Мера обеспечения информационной безопасности Распределение и использование привилегированных прав доступа следует ограничивать и контролировать
А.9.2.4	Процесс управления секретной аутентификационной информацией пользователей	Мера обеспечения информационной безопасности Предоставление секретной аутентификационной информации должно контролироваться посредством формального процесса управления.
А.9.2.5	Пересмотр прав доступа пользователей	Мера обеспечения информационной безопасности Владельцы активов должны регулярно пересматривать права доступа пользователей
А.9.2.6	Аннулирование или корректировка прав доступа	Мера обеспечения информационной безопасности Права доступа всех работников и внешних пользователей к информации и средствам ее обработки должны быть аннулированы (после их увольнения, истечения срока действия договора или соглашения) либо скорректированы в случае необходимости
А.9.3 Ответственность пользователей Цель: установить ответственность пользователей за защиту их аутентификационной информации		
А.9.3.1	Использование секретной аутентификационной информации	Мера обеспечения информационной безопасности При использовании секретной аутентификационной информации пользователи должны выполнять установленные в организации правила
А.9.4 Управление доступом к системам и приложениям Цель: предотвратить несанкционированный доступ к системам и приложениям.		
А.9.4.1	Ограничение доступа к информации	Мера обеспечения информационной безопасности Доступ к информации и функциям прикладных систем должен быть ограничен в соответствии с политикой управления доступом
А.9.4.2	Безопасные процедуры входа в систему	Мера обеспечения информационной безопасности Когда этого требует политика управления доступом, доступ к системам и приложениям должен управляться посредством безопасной процедуры входа в систему
А.9.4.3	Система управления паролями	Мера обеспечения информационной безопасности Системы управления паролями должны быть интерактивными и должны обеспечивать уверенность в качестве паролей
А.9.4.4	Использование привилегированных служебных программ	Мера обеспечения информационной безопасности Использование служебных программ, которые могли бы обойти меры обеспечения информационной безопасности систем и приложений, следует ограничивать и строго контролировать
А.9.4.5	Управление доступом к исходному тексту программы	Мера обеспечения информационной безопасности Доступ к исходному тексту программы должен быть ограничен

ГОСТ Р ИСО/МЭК 27001—2021

Продолжение таблицы А. 1

А.10 Криптография		
А.10.1 Криптографическая защита информации Цель: обеспечить уверенность в надлежащем и эффективном использовании криптографии для защиты конфиденциальности, подлинности (аутентичности) и/или целостности информации		
А.10.1.1	Политика использования криптографических мер и средств защиты информации	<i>Мера обеспечения информационной безопасности</i> Должна быть разработана и внедрена политика использования криптографических мер и средств для обеспечения защиты информации
А.10.1.2	Управление ключами	<i>Мера обеспечения информационной безопасности</i> Политика, определяющая использование, защиту и срок службы криптографических ключей, должна быть разработана и применяться на протяжении всего их жизненного цикла
А.11 Физическая безопасность и защита от воздействия окружающей среды		
А.11.1 Зоны безопасности Цель: предотвратить несанкционированный физический доступ, повреждение и воздействие на информацию организации и средства ее обработки		
А.11.1.1	Физический периметр безопасности	<i>Мера обеспечения информационной безопасности</i> Должны быть определены и использованы периметры безопасности для защиты зон, содержащих чувствительную или критическую информацию и средства ее обработки
А.11.1.2	Меры и средства контроля и управления физическим доступом	<i>Мера обеспечения информационной безопасности</i> Зоны безопасности должны быть защищены соответствующими мерами и средствами контроля доступа, чтобы обеспечить уверенность в том, что доступ разрешен только уполномоченному персоналу
А.11.1.3	Безопасность зданий, помещений и оборудования	<i>Мера обеспечения информационной безопасности</i> Должна быть разработана и реализована физическая защита зданий, помещений и оборудования
А.11.1.4	Защита от внешних угроз и угроз со стороны окружающей среды	<i>Мера обеспечения информационной безопасности</i> Должны быть разработаны и реализованы меры физической защиты от стихийных бедствий, злоумышленных атак или аварий
А.11.1.5	Работа в зонах безопасности	<i>Мера обеспечения информационной безопасности</i> Должны быть разработаны и применены процедуры для работы в зонах безопасности
А.11.1.6	Зоны погрузки и разгрузки	<i>Мера обеспечения информационной безопасности</i> Места доступа, например зоны погрузки и разгрузки, и другие места, где неуполномоченные лица могут проникать в помещения, должны находиться под контролем и, по возможности, должны быть изолированы от средств обработки информации во избежание несанкционированного доступа к ним
А.11.2 Оборудование Цель: предотвратить потерю, повреждение, хищение или компрометацию активов и прерывание деятельности организации		
А.11.2.1	Размещение и защита оборудования	<i>Мера обеспечения информационной безопасности</i> Оборудование должно быть размещено и защищено таким образом, чтобы снизить риски информационной безопасности от угроз и опасностей со стороны окружающей среды и возможности несанкционированного доступа
А.11.2.2	Вспомогательные услуги	<i>Мера обеспечения информационной безопасности</i> Оборудование должно быть защищено от сбоев электропитания и других сбоев, вызванных отказами в предоставлении вспомогательных услуг

ГОСТ Р ИСО/МЭК 27001—2021

Продолжение таблицы А. 1

A.11.2.3	Безопасность кабельной сети	<i>Мера обеспечения информационной безопасности</i> Кабели питания и телекоммуникационные кабели, используемые для передачи данных или для поддержки информационных сервисов, должны быть защищены от перехвата информации, помех или повреждения
A.11.2.4	Техническое обслуживание оборудования	<i>Мера обеспечения информационной безопасности</i> Должно проводиться надлежащее техническое обслуживание оборудования для обеспечения его непрерывной доступности и целостности
A.11.2.5	Перемещение активов	<i>Мера обеспечения информационной безопасности</i> Вынос оборудования, информации или программного обеспечения за пределы площадки эксплуатации без предварительного разрешения необходимо исключить
A.11.2.6	Безопасность оборудования и активов вне помещений организации	<i>Мера обеспечения информационной безопасности</i> Следует обеспечивать безопасность активов вне помещений организации, учитывая различные риски информационной безопасности, связанные с работой вне помещений организации
A.11.2.7	Безопасная утилизация или повторное использование оборудования	<i>Мера обеспечения информационной безопасности</i> Все компоненты оборудования, содержащие носители данных, необходимо проверять с целью обеспечения уверенности, что вся защищаемая информация и лицензионное программное обеспечение были удалены или перезаписаны безопасным образом до утилизации или повторного использования этих компонентов оборудования
A.11.2.8	Оборудование, оставленное пользователем без присмотра	<i>Мера обеспечения информационной безопасности</i> Пользователи должны обеспечить соответствующую защиту оборудования, оставленного без присмотра
A.11.2.9	Политика «чистого стола» и «чистого экрана»	<i>Мера обеспечения информационной безопасности</i> Должна быть принята политика «чистого стола» в отношении бумажных документов и сменных носителей информации, а также политика «чистого экрана» для средств обработки информации
A.12 Безопасность при эксплуатации		
A.12.1 Эксплуатационные процедуры и обязанности		
Цель: обеспечить надлежащую и безопасную эксплуатацию средств обработки информации		
A.12.1.1	Документально оформленные эксплуатационные процедуры	<i>Мера обеспечения информационной безопасности</i> Эксплуатационные процедуры должны быть документированы и доступны всем нуждающимся в них пользователям
A.12.1.2	Процесс управления изменениями	<i>Мера обеспечения информационной безопасности</i> Необходимо обеспечить управление изменениями в организации, бизнес-процессах, средствах обработки информации и системах, влияющих на информационную безопасность
A.12.1.3	Управление производительностью	<i>Мера обеспечения информационной безопасности</i> Необходимо осуществлять мониторинг, корректировку и прогнозирование использования ресурсов, исходя из будущих требований к производительности, для обеспечения требуемой производительности системы
A.12.1.4	Разделение сред разработки, тестирования и эксплуатации	<i>Мера обеспечения информационной безопасности</i> Для снижения рисков несанкционированного доступа или изменений среды эксплуатации необходимо обеспечивать разделение сред разработки, тестирования и эксплуатации

ГОСТ Р ИСО/МЭК 27001—2021

Продолжение таблицы А. 1

А.12.2 Защита от вредоносных программ Цель: обеспечивать уверенность в защите информации и средств обработки информации от вредоносных программ		
А.12.2.1	Меры обеспечения информационной безопасности в отношении вредоносных программ	<i>Мера обеспечения информационной безопасности</i> Для защиты от вредоносных программ должны быть реализованы меры обеспечения информационной безопасности, связанные с обнаружением, предотвращением и восстановлением, в сочетании с соответствующим информированием пользователей
А.12.3 Резервное копирование Цель: обеспечить защиту от потери данных		
А.12.3.1	Резервное копирование информации	<i>Мера обеспечения информационной безопасности</i> В соответствии с политикой резервирования следует регулярно создавать и проверять резервные копии информации, программного обеспечения и образов системы
А.12.4 Регистрация и мониторинг Цель: регистрация событий информационной безопасности и формирование свидетельств		
А.12.4.1	Регистрация событий	<i>Мера обеспечения информационной безопасности</i> Требуется обеспечивать формирование, ведение и регулярный анализ регистрационных журналов, фиксирующих действия пользователей, нештатные ситуации, ошибки и события информационной безопасности
А.12.4.2	Защита информации регистрационных журналов	<i>Мера обеспечения информационной безопасности</i> Средства регистрации и информация регистрационных журналов должны быть защищены от фальсификации и несанкционированного доступа
А.12.4.3	Регистрационные журналы действий администратора и оператора	<i>Мера обеспечения информационной безопасности</i> Действия системного администратора и оператора системы следует регистрировать, а регистрационные журналы защищать и регулярно анализировать
А.12.4.4	Синхронизация часов	<i>Мера обеспечения информационной безопасности</i> Часы всех систем обработки информации в рамках организации или домена безопасности должны быть синхронизированы с единым эталонным источником времени
А.12.5 Контроль программного обеспечения, находящегося в эксплуатации Цель: обеспечить уверенность в целостности систем, находящихся в эксплуатации		
А.12.5.1	Установка программного обеспечения в эксплуатируемых системах	<i>Мера обеспечения информационной безопасности</i> Должны быть реализованы процедуры контроля установки программного обеспечения в системах, находящихся в эксплуатации
А.12.6 Менеджмент технических уязвимостей Цель: предотвратить использование технических уязвимостей		
А.12.6.1	Процесс управления техническими уязвимостями	<i>Мера обеспечения информационной безопасности</i> Должна быть своевременно получена информация о технических уязвимостях используемых информационных систем, оценена подверженность организации таким уязвимостям, и должны быть приняты соответствующие меры в отношении связанного с этим риска информационной безопасности
А.12.6.2	Ограничения на установку программного обеспечения	<i>Мера обеспечения информационной безопасности</i> Должны быть установлены и реализованы правила, регулирующие установку программного обеспечения пользователями

ГОСТ Р ИСО/МЭК 27001—2021

Продолжение таблицы А. 1

А.12.7 Особенности аудита информационных систем Цель: минимизировать влияние аудиторской деятельности на функционирование систем, находящихся в эксплуатации		
А.12.7.1	Меры обеспечения информационной безопасности в отношении аудита информационных систем	<i>Мера обеспечения информационной безопасности</i> Требования к процессу регистрации событий (аудиту) и деятельности, связанной с контролем находящихся в эксплуатации систем, должны быть тщательно спланированы и согласованы для минимизации сбоев в бизнес-процессах
А.13 Безопасность системы связи		
А.13.1 Менеджмент безопасности сетей Цель: обеспечить защиту информации в сетях и в образующих их средствах обработки информации		
А.13.1.1	Меры обеспечения информационной безопасности для сетей	<i>Мера обеспечения информационной безопасности</i> Сети должны управляться и контролироваться для обеспечения защиты информации систем и приложений
А.13.1.2	Безопасность сетевых сервисов	<i>Мера обеспечения информационной безопасности</i> Механизмы обеспечения безопасности, уровни обслуживания и требования к управлению для всех сетевых сервисов должны быть идентифицированы и включены в соглашения по сетевым сервисам независимо от того, будут ли они обеспечиваться силами организации или осуществляться с использованием аутсорсинга
А.13.1.3	Разделение в сетях	<i>Мера обеспечения информационной безопасности</i> Группы информационных сервисов, пользователей и информационных систем в сети должны быть разделены
А.13.2 Передача информации Цель: поддерживать безопасность информации, передаваемой как внутри организации, так и при обмене с любым внешним объектом и субъектом		
А.13.2.1	Политики и процедуры передачи информации	<i>Мера обеспечения информационной безопасности</i> Должны существовать формализованные политики и процедуры передачи информации, а также соответствующие меры обеспечения информационной безопасности, обеспечивающие защиту информации, передаваемой с использованием всех видов средств связи
А.13.2.2	Соглашения о передаче информации	<i>Мера обеспечения информационной безопасности</i> Безопасная передача деловой информации между организацией и внешними сторонами должна быть определена соглашениями
А.13.2.3	Электронный обмен сообщениями	<i>Мера обеспечения информационной безопасности</i> Следует обеспечивать соответствующую защиту информации при электронном обмене сообщениями
А.13.2.4	Соглашения о конфиденциальности или неразглашении	<i>Мера обеспечения информационной безопасности</i> Требования в отношении соглашений о конфиденциальности или неразглашении, отражающие потребности организации в обеспечении защиты информации, должны быть идентифицированы, документально оформлены и регулярно пересматриваться
А.14 Приобретение, разработка и поддержка систем		
А.14.1 Требования к безопасности информационных систем Цель: обеспечить уверенность в том, что информационная безопасность является неотъемлемой частью информационных систем на протяжении всего их жизненного цикла. Это также включает требования к информационным системам, предоставляющим услуги с использованием сетей общего пользования		
А.14.1.1	Анализ и спецификация требований информационной безопасности	<i>Мера обеспечения информационной безопасности</i> Требования, относящиеся к информационной безопасности, должны быть включены в перечень требований для новых информационных систем или для усовершенствования существующих информационных систем

ГОСТ Р ИСО/МЭК 27001—2021

Продолжение таблицы А. 1

A.14.1.2	Обеспечение безопасности прикладных сервисов, предоставляемых с использованием сетей общего пользования	<i>Мера обеспечения информационной безопасности</i> Информация, используемая в прикладных сервисах и передаваемая по сетям общего пользования, должна быть защищена от мошеннической деятельности, оспаривания договоров, а также несанкционированного раскрытия и модификации
A.14.1.3	Защита транзакций прикладных сервисов	<i>Мера обеспечения информационной безопасности</i> Информацию, используемую в транзакциях прикладных сервисов, следует защищать для предотвращения неполной передачи, ложной маршрутизации, несанкционированного изменения, раскрытия, дублирования или воспроизведения сообщений
A.14.2 Безопасность в процессах разработки и поддержки Цель: обеспечить уверенность в том, что меры обеспечения информационной безопасности спроектированы и внедрены на всех стадиях жизненного цикла разработки информационных систем		
A.14.2.1	Политика безопасной разработки	<i>Мера обеспечения информационной безопасности</i> Правила разработки программного обеспечения и систем должны быть установлены и применены к разработкам в рамках организации
A.14.2.2	Процедуры управления изменениями системы	<i>Мера обеспечения информационной безопасности</i> Необходимо управлять изменениями в системах в течение жизненного цикла разработки посредством применения формализованных процедур управления изменениями
A.14.2.3	Техническая экспертиза приложений (прикладных программ) после изменений операционной платформы	<i>Мера обеспечения информационной безопасности</i> При внесении изменений в операционные платформы критически важные для бизнеса приложения должны быть проверены и протестированы, чтобы обеспечить уверенность в отсутствии неблагоприятного воздействия на деятельность или безопасность организации
A.14.2.4	Ограничения на изменения пакетов программ	<i>Мера обеспечения информационной безопасности</i> Следует избегать модификаций пакетов программ, ограничиваясь необходимыми изменениями, и строго контролировать все изменения
A.14.2.5	Принципы безопасного проектирования систем	<i>Мера обеспечения информационной безопасности</i> Принципы безопасного проектирования систем должны быть установлены, документированы, поддерживаться и применяться к любым работам по реализации информационной системы
A.14.2.6	Безопасная среда разработки	<i>Мера обеспечения информационной безопасности</i> Организация должна установить и надлежащим образом защищать безопасные среды разработки, используемые для разработки и интеграции систем на всех стадиях жизненного цикла разработки системы
A.14.2.7	Разработка с использованием аутсорсинга	<i>Мера обеспечения информационной безопасности</i> Организация должна осуществлять надзор и мониторинг разработки систем, выполняемой подрядчиками
A.14.2.8	Тестирование безопасности систем	<i>Мера обеспечения информационной безопасности</i> Тестирование функциональных возможностей безопасности должно осуществляться в процессе разработки
A.14.2.9	Приемо-сдаточные испытания системы	<i>Мера обеспечения информационной безопасности</i> Для новых информационных систем, обновлений и новых версий должны быть разработаны программы приемо-сдаточных испытаний и установлены связанные с ними критерии
A.14.3 Тестовые данные Цель: обеспечить защиту данных, используемых для тестирования		
A.14.3.1	Защита тестовых данных	<i>Мера обеспечения информационной безопасности</i> Тестовые данные следует тщательно выбирать, защищать и контролировать

ГОСТ Р ИСО/МЭК 27001—2021

Продолжение таблицы А. 1

А.15 Взаимоотношения с поставщиками		
А.15.1 Информационная безопасность во взаимоотношениях с поставщиками Цель: обеспечить защиту активов организации, доступных поставщикам		
А.15.1.1	Политика информационной безопасности во взаимоотношениях с поставщиками	<i>Мера обеспечения информационной безопасности</i> Требования информационной безопасности, направленные на снижение рисков, связанных с доступом поставщиков к активам организации, должны быть согласованы с поставщиком и документированы
А.15.1.2	Рассмотрение вопросов безопасности в соглашениях с поставщиками	<i>Мера обеспечения информационной безопасности</i> Все соответствующие требования информационной безопасности должны быть установлены и согласованы с каждым поставщиком, который может получить доступ к информации организации, обрабатывать, хранить, передавать информацию или предоставлять соответствующие компоненты ИТ-инфраструктуры
А.15.1.3	Цепочка поставок информационно-коммуникационной технологии	<i>Мера обеспечения информационной безопасности</i> Соглашения с поставщиками должны содержать требования по рассмотрению рисков информационной безопасности, связанных с цепочкой поставок продуктов и услуг информационно-коммуникационных технологий
А.15.2 Управление услугами, предоставляемыми поставщиком Цель: поддерживать согласованный уровень информационной безопасности и предоставления услуг в соответствующих соглашениях с поставщиками		
А.15.2.1	Мониторинг и анализ услуг поставщика	<i>Мера обеспечения информационной безопасности</i> Организация должна регулярно проводить мониторинг, проверку и аудит деятельности поставщика по предоставлению услуг
А.15.2.2	Управление изменениями услуг поставщика	<i>Мера обеспечения информационной безопасности</i> Требуется управлять изменениями в предоставляемых поставщиками услугах, включая поддержку и улучшение существующих политик, процедур, а также мер и средств информационной безопасности, с учетом категории информации бизнеса, задействованных систем и процессов, а также результатов переоценки рисков информационной безопасности
А.16 Менеджмент инцидентов информационной безопасности		
А.16.1 Менеджмент инцидентов информационной безопасности и улучшений Цель: обеспечить последовательный и эффективный подход к менеджменту инцидентов информационной безопасности, включая обмен информацией о событиях безопасности и недостатках		
А.16.1.1	Обязанности и процедуры	<i>Мера обеспечения информационной безопасности</i> Должны быть установлены обязанности и процедуры менеджмента для обеспечения уверенности в быстром, эффективном и надлежащем реагировании на инциденты информационной безопасности
А.16.1.2	Сообщения о событиях информационной безопасности	<i>Мера обеспечения информационной безопасности</i> Требуется как можно скорее сообщать о событиях информационной безопасности по соответствующим каналам управления
А.16.1.3	Сообщения о недостатках информационной безопасности	<i>Мера обеспечения информационной безопасности</i> Работники и подрядчики, использующие информационные системы и услуги организации, должны обращать внимание на любые замеченные или предполагаемые недостатки информационной безопасности в системах или сервисах и сообщать о них
А.16.1.4	Оценка и принятие решений в отношении событий информационной безопасности	<i>Мера обеспечения информационной безопасности</i> Должна быть проведена оценка событий информационной безопасности, и должно быть принято решение, следует ли их классифицировать как инциденты информационной безопасности

ГОСТ Р ИСО/МЭК 27001—2021

Продолжение таблицы А. 1

A.16.1.5	Реагирование на инциденты информационной безопасности	<i>Мера обеспечения информационной безопасности</i> Реагирование на инциденты информационной безопасности должно осуществляться в соответствии с документально оформленными процедурами
A.16.1.6	Анализ инцидентов информационной безопасности	<i>Мера обеспечения информационной безопасности</i> Знания, приобретенные в результате анализа и урегулирования инцидентов информационной безопасности, должны использоваться для уменьшения вероятности или влияния будущих инцидентов
A.16.1.7	Сбор свидетельств	<i>Мера обеспечения информационной безопасности</i> В организациях должны быть определены и применяться процедуры для идентификации, сбора, получения и сохранения информации, которая может использоваться в качестве свидетельств
А.17 Аспекты информационной безопасности в рамках менеджмента непрерывности деятельности организации		
А.17.1 Непрерывность информационной безопасности Цель: непрерывность обеспечения информационной безопасности должна быть неотъемлемой частью систем менеджмента непрерывности деятельности организации		
A.17.1.1	Планирование непрерывности информационной безопасности	<i>Мера обеспечения информационной безопасности</i> Организация должна определить свои требования к информационной безопасности и менеджменту непрерывности информационной безопасности при неблагоприятных ситуациях, например во время кризиса или бедствия
A.17.1.2	Реализация непрерывности информационной безопасности	<i>Мера обеспечения информационной безопасности</i> Организация должна устанавливать, документировать, реализовывать и поддерживать процессы, процедуры, а также меры обеспечения требуемого уровня непрерывности информационной безопасности при неблагоприятных ситуациях
A.17.1.3	Проверка, анализ и оценивание непрерывности информационной безопасности	<i>Мера обеспечения информационной безопасности</i> Организация должна регулярно проверять установленные и реализованные меры обеспечения непрерывности информационной безопасности, чтобы обеспечить уверенность в их актуальности и эффективности при возникновении неблагоприятных ситуаций
А. 17.2 Резервирование оборудования Цель: обеспечить уверенность в доступности средств обработки информации		
A.17.2.1	Доступность средств обработки информации	<i>Мера обеспечения информационной безопасности</i> Средства обработки информации должны быть внедрены с учетом резервирования, достаточного для выполнения требований доступности
А.18 Соответствие		
А.18.1 Соответствие правовым и договорным требованиям Цель: избежать нарушений правовых и регулятивных требований или договорных обязательств, связанных с информационной безопасностью, и других требований безопасности		
A.18.1.1	Идентификация применимых законодательных и договорных требований	<i>Мера обеспечения информационной безопасности</i> Все значимые для организации и каждой информационной системы правовые, регулятивные и договорные требования, а также подходы организации к выполнению этих требований должны быть четко определены, документированы и поддерживаться в актуальном состоянии как в отношении каждой информационной системы, так и в отношении организации в целом

ГОСТ Р ИСО/МЭК 27001—2021

Окончание таблицы А. 1

A.18.1.2	Права на интеллектуальную собственность	<i>Мера обеспечения информационной безопасности</i> Должны быть реализованы соответствующие процедуры для обеспечения уверенности в соблюдении правовых, регулятивных и договорных требований, связанных с правами на интеллектуальную собственность и правами использования проприетарных программных продуктов
A.18.1.3	Защита записей	<i>Мера обеспечения информационной безопасности</i> Записи должны быть защищены от потери, уничтожения, фальсификации, несанкционированного доступа и разглашения, в соответствии с правовыми, регулятивными, договорными и бизнес-требованиями
A.18.1.4	Конфиденциальность и защита персональных данных	<i>Мера обеспечения информационной безопасности</i> Конфиденциальность и защита персональных данных должна обеспечиваться в соответствии с требованиями соответствующего законодательства и правилами там, где это применимо
A.18.1.5	Регулирование криптографических мер и средств защиты информации	<i>Мера обеспечения информационной безопасности</i> Криптографические меры обеспечения информационной безопасности должны использоваться с соблюдением требований всех соответствующих соглашений, правовых и регулятивных актов
A.18.2 Проверки информационной безопасности Цель: обеспечить уверенность в том, что информационная безопасность реализована и эксплуатируется в соответствии с политикой и процедурами организации		
A.18.2.1	Независимая проверка информационной безопасности	<i>Мера обеспечения информационной безопасности</i> Подход организации к менеджменту информационной безопасностью и ее реализация (т. е. цели, меры и средства, политики, процессы и процедуры информационной безопасности) следует проверять независимо друг от друга через запланированные интервалы времени или в случае значительных изменений
A.18.2.2	Соответствие политикам и стандартам безопасности	<i>Мера обеспечения информационной безопасности</i> Руководители, в пределах своей зоны ответственности, должны регулярно проверять соответствие процессов и процедур обработки информации соответствующим политикам безопасности, стандартам и другим требованиям безопасности
A.18.2.3	Анализ технического соответствия	<i>Мера обеспечения информационной безопасности</i> Информационные системы должны регулярно проверяться на предмет соответствия стандартам и политикам информационной безопасности организации

ГОСТ Р ИСО/МЭК 27001—2021

Приложение ДА
(справочное)Сведения о соответствии ссылочных международных стандартов
национальным стандартам

Таблица ДА. 1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование ссылочного национального стандарта
ISO/IEC 27000	IDT	ГОСТ Р ИСО/МЭК 27000—2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

ГОСТ Р ИСО/МЭК 27001—2021

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

ГОСТ Р ИСО/МЭК 27001—2021

УДК 006.035:004.056.5:004.057.2:006.354

ОКС 35.040

Ключевые слова: обеспечение информационной безопасности, система менеджмента информационной безопасности, политика информационной безопасности, требование по обеспечению информационной безопасности, мера обеспечения информационной безопасности

Редактор *Л.В. Каретникова*
Технический редактор *И.Е. Черепкова*
Корректор *Л. С. Лысенко*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 02.12.2021. Подписано в печать 27.12.2021. Формат 60х84%. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,95. Тираж 22 экз. Зак. 1591.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано в ФГБУ «РСТ»
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru